(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/93000 A2

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US01/16821

(22) International Filing Date: 23 May 2001 (23.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/584,134 31 May 2000 (31.05.2000) US

(71) Applicant: ZORAN CORPORATION [US/US]; 3112 Scott Boulevard, Santa Clara, CA 95054 (US).

(72) Inventors: GOLDBERG, Paul, R.; 744 La Para Avenue, Palo Alto, CA 94306 (US). NEIDICH, Michael; 444 Saratoga Avenue, Santa Clara, CA 95050 (US).

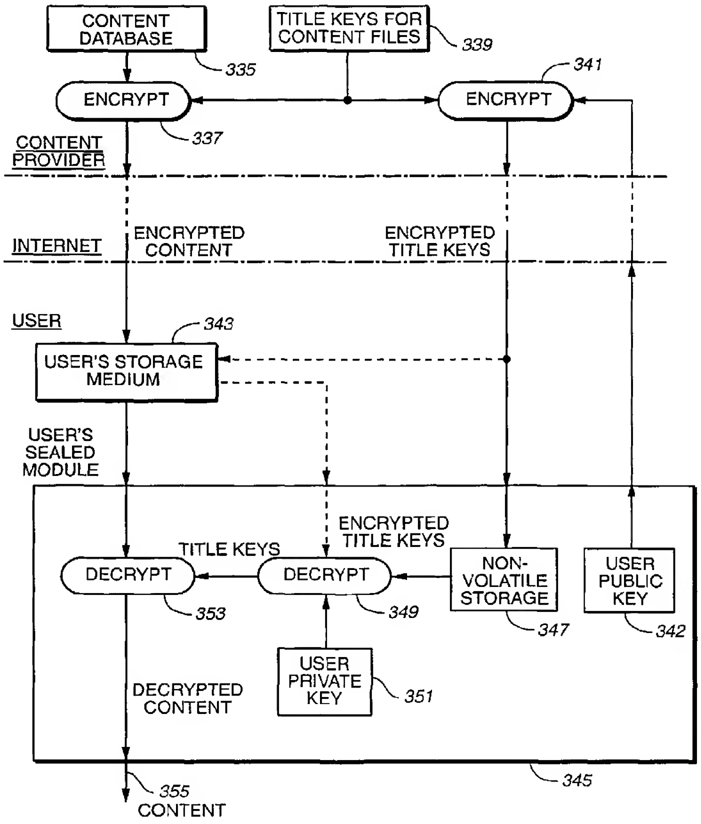
(74) Agent: PARSONS, Gerald, P.; Skjerven Morrill Macpherson, LLP, Three Embarcadero Center, 28th Floor, San Francisco, CA 94111 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE ELECTRONIC INTERNET DELIVERY AND USE OF MUSIC AND OTHER VALUABLE DATA



(57) Abstract: Techniques of transferring digital data, such as that of music, over a communications network, such as the Internet, wherein an identification code supplied by the recipient or the recipient's utilization device, such as a computer or a device that utilizes the data, to the data provider is used to encrypt the data and send it to the recipient. A utilization device of the recipient, such as a music player, then decrypts the data by use of either the same identification code as a key or another key that is related to the identification code. The decryption key is not accessible by the recipient or the recipient's computer or utilization device in an unencrypted form. Access to the transferred data in an unencrypted form is prevented in order to prevent unauthorized copying and distribution of the data. Copies of the encrypted data file and the decryption key may be made for the recipient's use on multiple utilization devices without risking mass unauthorized copying and distribution.

WO 01/93000 A2

Published:

— *without international search report and to be republished upon receipt of that report*

SECURE ELECTRONIC INTERNET DELIVERY AND USE OF MUSIC AND OTHER VALUABLE DATA

BACKGROUND OF THE INVENTION

This invention relates generally to providing security in data transmission and distribution, and, more specifically, to techniques of restricting the use of valuable audio data, especially music, and video data to authorized persons or equipment.

Because of the rapid increase in the use of the Internet to transmit confidential information, efforts have been directed to make such data transmissions secure so that only the intended recipient or recipients can access the data. Data of documents being distributed within a company that contain trade secret information of that company that would be valuable to its competitors is an example. A typical security technique is to encrypt the data before transmission with a known encryption algorithm that requires a secret key to operate. The encryption algorithm is also possessed by the intended recipient. The key used to encrypt the data is then communicated by other means to the recipient, such as by telephone, who is then able to decrypt the data by inserting this key into the decryption algorithm. No one else can decrypt the data transmission unless they have the key used in its encryption by the sender.

Although this approach is generally satisfactory to prevent third parties from accessing the transmitted data of information that is of limited interest to others, it is not satisfactory for transmitting data over the Internet that could be mass distributed in digital form by a recipient given the means to decrypt the data and who is willing to violate the copyright of the provider. Digital data of music that is currently being distributed over the Internet is easily copied by a recipient and redistributed to friends and even sold in large numbers to the public. This is severely inhibiting music providers from distributing their products over the Internet. As the increasing bandwidth of the Internet increases over time, thus making it possible to distribute data of films and videos over the Internet, the same problem will exist. It is desirable, for a wide variety of digital data being transmitted over the Internet, to be able to control the recipients' ability to make and distribute copies of the digital data which is received.

SUMMARY OF THE INVENTION

According to the present invention, briefly and generally, data sent by the content provider to the recipient is encrypted by an encryption key that is initially supplied by the recipient. This encryption key is preferably specific to a computer or other utilization device of the recipient, or is personal to the recipient. The recipient's utilization device then decrypts the received encrypted data with a decryption key that is stored within the utilization device in a secure manner so as not to be accessible to the recipient or others. The decryption key is either the same as the encryption key, or they are related in some operative manner. The encryption of the transmitted data is then personal to the recipient or the recipient's utilization device. Not only does this provide a high level of security against anyone intercepting the transmission being able to decrypt the data, it is more difficult for the recipient to unlawfully distribute copies of unencrypted digital data because the decryption key is unknown to the recipient.

According to a first general embodiment, the decryption key is stored in a secure manner in the recipient's utilization device and the same key is used by the content provider to encrypt the content data before sending it to the recipient. This key is sent to the content provider by the recipient's utilization device in an encrypted form.

According to a second general embodiment, the encryption key sent by the recipient's utilization device is a public key that need not be first encrypted since the decryption key is a private one that is stored in the recipient's utilization device in a manner to be inaccessible except by the internal signal processor. The public and private keys are related so that a data file encrypted by the content provider with the known public key can be decrypted by the inaccessible private key.

According to a third general embodiment, the data files are individually encrypted by the content user with unique title keys but the title keys necessary to decrypt the content data files are transmitted to the recipient according to either of the foregoing first and second general embodiments. The recipient's utilization device first decrypts the title keys supplied by the content provider, and then uses the title keys to decrypt the content data files.

A current application of the techniques of the present invention is for the distribution and use of music in a digital form over the Internet communications network or any other electronic communications system. The utilization devices then provide an analog sound output generated from decrypted digital data. The utilization devices are preferably constructed in a manner that avoids generating an unencrypted version of the data file in binary form in a place or manner that is accessible to the user, in order to decrease the likelihood that unauthorized digital copies will be made from the received data that can be played on existing devices or transmitted over the Internet. Providing the analog sound output is unavoidable, since that is what is desired to be reproduced, but unauthorized copying of the reproduced sound will not give the high quality copy that copying of digital files will do. The decryption is preferably performed in a computer, audio player or other utilization device by a signal processor that is separate from the unit's central processor. Unencrypted digital data does not then appear on any internal processor bus. Rather, encrypted digital files are stored in a computer's hard disk, an audio player's removable memory card or other mass memory, and it is these encrypted files that are passed over an internal bus to the separate signal processor. This separate processor also has its own memory to store the decryption key and any other useful software or code. Any lines of the separate signal processor that carry the unencrypted digital data, if any, are mechanically sealed to make it very difficult for the computer user to access them. Thus, unencrypted digital data is practically not available to the computer user so is not available for making unauthorized copies.

According to another feature of the present invention, an analog signal output of a secure signal processor can be avoided. Rather than including a digital-to-analog converter as part of the signal processor, whose output is a good quality analog signal, a variable pulse width or repetition rate modulated signal of the type internally generated in high quality audio systems is generated by the processor instead. Such a signal cannot be copied by standard analog or digital recorders, and is of no use for sending over the Internet. Additional protection against misuse of received content data by unscrupulous recipients is thereby provided.

Although the goal in transferring digital files to the end user is to prevent, to the extent possible, unrestricted copying of unencrypted digital data, the user often has a legitimate need to make copies of the music, or other data, for his or her own use by reproduction on utilization devices other than the computer or other device which originally received and stored the encrypted data file. The user may freely copy the encrypted data files stored on his or her computer or other device and other aspects of the present invention pertain to allowing such copies to be played on other devices without making unencrypted digital data available for unauthorized copying. In order to allow a user to reproduce the content of an encrypted data file copy on several utilization devices to which the user has access, according to a first embodiment, additional encrypted identification codes can be sent to the content provider so that several such codes can all be used as keys in the encryption algorithm used to encrypt the data, thus enabling the data files to be decrypted on any utilization device having any one of the encrypted codes stored in its processor memory. In a second embodiment additional encrypted identification codes can be sent to the content provider so that a plurality of such codes can be used as keys in the encryption algorithm used to encrypt additional title keys, thus enabling the data files to be decrypted on any utilization device having any one of the encrypted codes stored in its processor memory. In a third embodiment, public encryption keys of several utilization devices to which the user has access can be sent to the content provider instead of encrypted identification codes. As in the first embodiment, this permits several such public keys to be used as keys in the encryption algorithm, thus enabling the data files to be decrypted on any utilization devices having any one of the private keys associated with these public keys stored in the processor memory. In a fourth embodiment, public encryption keys of several utilization devices to which the user has access can be sent to the content provider instead of encrypted identification codes. As in the second embodiment, this permits several such public keys to be used as keys in the encryption algorithm employed to encrypt additional title keys, thus enabling the data files to be decrypted on any utilization devices having any one of the private keys associated with these public keys stored in the processor memory. In a fifth embodiment, the decryption key is made to be portable in order to enable the user to transfer that key, along with the music or other data content to be played, to any available utilization device. This is accomplished, in one specific form, by forming the decryption signal processor and its non-volatile memory on a separate card personal to the holder that is removably connectable with a wide variety of utilization devices. This enables its holder to decrypt and play data files on any compatible utilization device. An individual user then needs to posses only one identification code to act as a key to decryption of the data files that are playable on a number of devices.

The various features of the present invention summarized above may individually be employed, with the result of increasing the difficulty of a recipient who is intent on mass distributing copies of the data in an unencrypted digital form. However, a combination of these individual features significantly increases the level of security. Additional objects, features and advantages of the various aspects of the present invention are included in the following description of some specific embodiments, which description should be taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 schematically illustrates one embodiment of a secure data communications and utilization system;

Figure 2 is a block diagram of the communication and content interface block of Figure 1;

Figure 3 is a block diagram of a data utilization system that supplements that of Figures 1 and 2;

Figure 4 illustrates an audio player system as a utilization device according to another embodiment of a secure data communications and utilization system;

Figure 5 shows an example of a key card used in the system of Figure 4;

Figure 6 is a block electronic diagram of the system of Figure 4;

Figure 7 illustrates example contents of a read-only memory within the system of Figures 4-6;

Figure 8 is a diagram showing a process performed by the system of Figures 4-6 to generate encryption and decryption keys specific to a particular system or its user;

Figure 9 illustrates example contents of another read-only memory within the system of Figure 4-6;

Figure 10 shows the contents of an example data file received by the system of Figures 4-9;

Figure 11 is a flow chart that outlines an example technique for the system of Figures 4-10 to obtain encrypted digital data files;

Figure 12 is a flow chart that outlines an example technique for the system of Figures 4-10 to use obtained encrypted digital data files;

Figure 13 illustrates the flow of encryption keys and data between a content provider and an end user customer in the embodiment of Figures 4-12;

Figure 14 shows the use of a transcryptor to transfer content data in the form of the embodiment of Figures 4-12 from one user to another in a manner that the second user may play the data with his or her own keys;

Figure 15 illustrates the flow of encryption keys and content data between a content provider and an end user according to a further embodiment;

Figures 16A and 16B illustrate the contents of data files which can exist in the embodiment of Figure 15;

Figure 17 shows the use of a transcryptor to transfer content data in the form of the embodiment of Figure 15 from one user to another in a manner that the second user may play the data with his or her own keys;

Figure 18 illustrates the contents of a data file that can be generated by the transcryptor of Figure 17;

Figure 19 shows how content data acquired according to the embodiment of Figure 15 by multiple users can be played on a single utilization device;

Figure 20 illustrates the flow of encryption keys and content data through a distribution system from a content provider to and end user;

Figure 21 represents an optical disc storage medium in which encrypted data is stored; and

Figure 22 illustrates the transfer of decryption keys for authorizing the playing of selected content data files from a recording of a very large number of files.

DESCRIPTION OF EMBODIMENTS OF THE INVENTION

Referring initially to Figure 1, a computer 11 of person desiring to receive one or more digital data files is connected through a communications network 15, such as the Internet, by lines 14 and 16, to a computer 13, at a different location, that provides specified digital files to the user's computer 11 in response to the user making a request through his or her computer 11. In this description, the example of distributing music digital data files over the Internet is described but the techniques are equally applicable to the distribution of other audio or video digital data files, including those of still pictures, as well as files having other content. Although this description is directed to the reproduction of analog signals from the acquired data files, the invention is not so limited.

The computer 11 of the desired recipient of a data file from the provider 13 contains many parts common to most personal computers. A number of components are connected to and communicate with each other over an internal bus 17. A central processing unit (CPU) 19 is also connected with a main memory 21, usually dynamic random access memory (DRAM), and a read only memory (ROM) 23. A mass data storage device 25, usually a hard disk system, is also connected to the bus 17. Various peripherals illustrated in Figure 1 include a video card 27 that provides video signals to a monitor 29, most commonly a cathode-ray-tube (CRT) or liquid crystal display (LCD) type of monitor. A keyboard and mouse, indicated at 31, are also connected to the bus 17, as is an audio card 33 that drives an internal loud speaker 34.

One or more removable media type of storage devices 35 are also included in the computer 11, with a removable medium 37 being illustrated. The removable medium 37 can be magnetic, such as a floppy disc or a magnetic disc of larger capacity that is currently commercially available, an optical compact disc (CD ROM), or a non-volatile semiconductor memory card. Two or more storage devices 35 of different types are typically included in a personal computer. Such devices 35 can be limited to read the digital data from their respective media 37 but more commonly also have the ability to write data to those media.

A circuit 39 connected with the bus 17, preferably provided on a separate printed circuit card installed in the computer 11, interfaces with the Internet 15 through the lines 14. The circuit 39 also outputs an analog music signal from a received data file over line 41 that drive an analog device 43, in this example an audio device that drives one or more loud speakers 45. The analog device 43 typically includes ordinary commercially available audio equipment. That equipment can be chosen to reproduce any stereo or multi-channel signals of its input signal in the line 41, and can contain decoders or the like of those signals that are currently available in various types of audio equipment. The audio signal in the line 41 preferably has the same format as the output from current audio compact disk players, so simply provides one more input source to a typical home or business audio system.

In addition to communicating with the remote content provider 13 to obtain encrypted data files from it, the interface card 39 has the purpose of decrypting these data files and generating the analog signal output 41. An encrypted data file is preferably stored in the computer disk drive, or other type of mass storage 25, as it is received from the provider 13. This file is then later read from the hard disk and processed by the card 39 to decrypt the data file and convert it into an analog form. This is preferred to having the CPU 19 perform the decryption since it avoids transmitting the decrypted file over the computer bus 17 and other components where it can rather easily be accessed by a user who desires to produce digital copies of the data file in violation of the provider's copyright.

An example of the interface card 39 is given in Figure 2. Interface circuits 55 will usually include a high speed modem for communicating over the Internet through lines 14. The interface circuits 55 also provide a connection between a digital signal processor (DSP) 57 and either the internal bus 17, for receiving an encrypted data file previously stored on mass storage 25, or to the modem for processing a data file as it is being received over the Internet. In either case, the DSP 57 decrypts the data file, decompresses the file if it has been compressed by one of many audio compression algorithms, such as MPEG 1 Layer 3 (MP3), Advanced Audio Coding (AAC) or Dolby Digital (AC-3), and sends the decrypted, uncompressed data file to a digital-to-analog converter (DAC) 59 and a corresponding analog signal to audio output circuits 61, which contain pre-amplifiers and the like. Decrypted digital signals appear on the lines between the DSP 57 and the DAC 59, as well as on other lines interconnecting elements on the interface card 39. At least those lines, the circuit chips making up the DSP 57 and DAC 59, and integrated circuit chips forming a memory are encased by an encapsulant such as epoxy or the like to prevent access by the user to the decrypted digital signals or any stored decryption algorithms. This is done in a way that removal of the epoxy or other mechanical sealing material destroys the circuit lines and chips which are encased. An advantage of the system of Figures 1 and 2 is that this is the only place where such signals are available, thus making protection of the decrypted digital data easier to accomplish. If the DSP 57 and DAC 59 are combined into a single integrated circuit chip, this protection becomes even easier.

A non-volatile memory 63 on the interface card 39 includes several files used to remotely access and decrypt the data files. An identification code specific to the computer 11, or personal to its user, is stored in an encrypted form in a small file 65. It is not required that the identification code of every interface card 39 in use be different from any other, although that is preferable, but rather that any duplications of the code be few so that the probability of one computer being able to decrypt data files obtained by another computer is extremely remote. The identification code is preferably assigned by the manufacturer of the card 39 and not communicated to the user. The card manufacturer further encrypts the identification code before storing it in the file 65. Although the encrypted code 65 is made available for reading out from the memory 63 for transmission over the Internet, and thus can be read by the user, the algorithm for decrypting the file 65 is not so available.

When the user wants to access the content provider computer 13 to obtain a data file, his or her computer 11 sends the encrypted identification code from the file 65 over the Internet to the provider. The provider then decrypts this file to obtain the identification code assigned to the computer card 39. That identification code is then used as a key with an encryption algorithm that is used by the provider to encrypt the data file before sending it back over the Internet to the computer 11. The identification code is then decrypted on the board 39 for use in decrypting the received data file. The decryption algorithm is stored in a file 67 of the memory 63 and is made accessible by only the DSP 57 so the user cannot have access to it. This preserves the security of the identification code that is used to decrypt the received data file.

The data file decryption algorithm can be sent by the content provider along with the data file in an unencrypted manner. Security is provided by the content provider using the unknown identification code as a key in that encryption algorithm. Increased security is provided, however, if at least a portion of the decryption algorithm is stored as a file 68 in the memory 63, in a manner that it is accessible and readable only by the DSP 57. If a portion common to different specific algorithms used by different content providers is stored on the card 39, then the individual content providers are still free to chose their overall encryption algorithms so long as they use that common portion. The remaining portion of the decryption algorithm is then sent by the content provider along with the encrypted data file in an unsecured form.

When the DSP 39 is decrypting a received data file, it first utilizes the decryption algorithm of the file 67 to determine the card identification code. This identification code is then used as a key with the encryption algorithm portion of the file 68 along with any additional portions sent by the content provider with the encrypted data file to decrypt the received data file. The decrypted file is then converted into analog form and the resulting audio signal played through a sound system 43, 45. This decryption process occurs each time the analog audio content of a data file is played.

This avoids storing an unencrypted digital data file which presents a high risk of unauthorized copying and distribution.

On the content provider side of the Internet, a large computer 47 performs the encryption of data files stored in a large database 49 by means of encryption algorithms stored in a file 51. The file 51 includes the algorithm for decrypting the identification code sent by the computer 11 when requesting a data file, the data file encryption algorithm and any remaining portion of the data file decryption algorithm which is sent to the computer 11 along with the encrypted data file.

The portion of the memory 63 storing the decryption files 67 and 68 will usually be made from one time programmable read-only memory (ROM), since that is the easiest and most economical for mass production, particularly when the data is the same for all cards 39 being manufactured. Since the file 65 is different for each one of the cards 39, it may be optimal to use programmable flash memory for that file, although the one-time programmable ROM can also be used. In cases where the ability to change the encrypted code in the file 65 after manufacture, or to add additional encrypted identification codes to the file 65 is desired, a programmable non-volatile memory is preferred.

Because a music listener will likely not be satisfied to have to play the received data file through only the computer 11 that contains the identification code with which the music file was encrypted by the provider, some provision is desirable for the user to make copies for his or her own limited use on other playback devices. Any data file on the disk of the computer 11 may be copied to a removable medium of the removable media storage device 35. This copy is, of course, encrypted with the individual identification code of the card 39. There are several ways that can be alternatively implemented to allow the encrypted copy to be played on other utilization devices without significantly increasing the risk to the content provider that unencrypted digital files can be accessed.

An example of a playback device separate from the computer 11 is given in Figure 3. This device can be in any convenient format, an example being a small hand held playback device operated by batteries. Control circuits 71 receive the encrypted data file from a removable media storage device 73 in which a removable medium 75 containing the data file is inserted. Use of a small flash memory card for the medium 75 contributes to making the playback device very small and portable, if that is desired. The data file is then processed, decrypted and played in the same manner as described with respect to Figure 2. A DSP 77 receives decryption algorithms 89 and 90 from a non-volatile memory 85 for use in decrypting the received data file. Once decrypted, it is converted to an analog audio signal by a DAC 79 and that audio signal applied to audio amplifiers and other circuits 81 that drive a loud speaker or headphones. The structure and operation of the DSP 77, DAC 79 and the memory 85 are substantially the same as the respective components DSP 57, DAC 59 and memory 63 of the card 39 described with respect to Figure 2.

However, a significant difference is that the identification code for the device that is stored in an encrypted form in a file 87 of the memory 85 is not the same as the identification code used by the content provider to encrypt the data file. Each such device is manufactured with an identification code specific to that device. Thus, the playback device of Figure 3 cannot play back the content of that file in the manner described above for the card 39 without having access to the identification code used to encrypt the file that must be decrypted before it can be played. One way to overcome this is to provide for the computer 11 to copy the encrypted identification code file 65 from the card 39 onto the removable memory medium 75 along with the encrypted data file. The DSP 77 of the playback device of Figure 3 could then copy that encrypted identification code file from the storage medium 75 into its memory file 87 (with at least that portion of the memory 85 being re-writeable) for use by the DSP 77 to decrypt the data file on the medium 75 in the same manner as described above for the card 39. However, this does significantly increase the risk of further unauthorized multiple copies of the medium 75 being made since each copy would play on any playback device regardless of its unique identification.

Therefore, other approaches to the making and use of copies of encrypted data files are preferred. One is for the encrypted identification file of each computer having a card 39 and other playback devices possessed by a single user or group of users being transmitted to the content provider prior to the data file being encrypted by the provider. The requested data file is then encrypted by the content provider with each of the multiple identification codes as keys. The encrypted data file is then playable on any of the devices having those identification codes. In the case of the playback device of Figure 3, the control circuits 71 then include a modem for connection with the Internet in order to be able to transmit the encrypted identification code file 87 to the content provider. A preferred system has a particular user "register" with each desired content provider the encrypted identification code files from all his or her playback devices, so that all content subsequently ordered by that user will be encrypted with a key for decrypting by each device. The risk to the content of unauthorized copying and mass distribution by such a system remains low.

But this system of user copying does not allow existing copies possessed by the user to be played on a device that is acquired by the user after the data file is encrypted. One approach is to require the user to repurchase the same data files from the content provider who will now encrypt them with the keys used before plus an added key for the new device. Another approach is to provide for the encrypted identification code file 87 (Figure 3) of a new device to be written with another encrypted code from an old device possessed by the user. The copies that are properly decoded by the old device will then also be decoded by the new device after it receives the additional encrypted code file. The equipment is then designed to receive and store the additional encrypted code file in an authorized manner. It is not desirable to allow the user to freely copy those files from one device to another because of an increased risk to the security of the data files. Therefore, a system is set up whereby a content provider, the device manufacturer or the store from which the new device is purchased writes the encrypted code file from one device to another. A content provider preferably keeps such files of users who have previously purchased data files from it, so then transfers the necessary existing encrypted code file to the user's new device memory over the Internet. It may also be desirable to transfer content decryption algorithms to the additional playback devices that match the content to be played, particularly if there have been changes over time. Older utilization devices may also have the contents of their memories updated from time-to-time with changing decryption algorithms.

This technique of writing new encrypted code files to devices can optionally be extended to transferring the encrypted code files from playback devices of friends or relatives into all the playback devices of a user, thus allowing friends and relatives to exchange and play back encrypted data file copies. If this added capability is provided, however, the revenue of the content providers will decrease an amount corresponding to the number of sales that the copied data files replace. If the ability to make copies for personal use is restricted too much, however, distribution of music over the Internet may not become a significant business since users will not use the system very much.

Use of Blank Media with User's Identification Code Thereon

Another method of allowing limited copies to be made calls for the content providers, or others sharing their interest, to sell blank recordable memory media to users with a file of an encrypted user's identification code recorded on the media in a way that cannot be copied onto other such media but which is read by any playback device to decrypt the data file of music, or other content, that is later copied by the user onto the blank medium. Under this method, a user sends a request for blank media to a provider along with an encrypted identification code file or files to be written by the provider into the blank media that is then shipped to the user. The encrypted code file or files copied onto the blank media need to include those used to encrypt the data files that the user intends to copy onto the media. This will normally be the encrypted code file from the user's computer sending the request but is not limited to that. When the blank media is received, the user simply copies desired encrypted music data files onto them and then plays them back on any playback device. Useful physical media provided by content providers include compact disks or non-volatile semiconductor memory cards.

When this system is used, the interface card 39 and other players are caused to first look to that unique address of the medium for the encrypted identification code file and, if it exists, to decrypt it to obtain the key with which the music data file copied onto the medium has been encrypted. The playback device then decrypts the data file stored on the medium with this key in the same manner as previously described, and the music analog signals are obtained. If such an encrypted code file is not found at the designated address of the medium, the device then uses the encrypted code file(s) stored in the memory of the device. The copy is playable only if its data file was initially encrypted by the content provider with one of the identification codes stored on the medium or in the utilization device that is decrypting the data. This then allows a user to play such copies on any compatible device, while the content provider has been compensated for providing the blank media with the users identification code(s) to the user.

The provider writes the encrypted identification code file(s) on the blank media being purchased in a manner that practically prevents copying of that file(s) by others from the purchased media onto other media. If the media are optical compact disks, the encrypted code file(s) are written on the disks in a track provided by disk manufactures for writing only by a laser having a power level much higher than those available in consumer recordable compact disk equipment. Therefore, although the encrypted code file can be read, it cannot be written by the user in the same track on copies made from the purchased disks. Consumer optical disk writing devices do not have lasers with sufficient power to write data in this area. Non-programmable addresses of flash semiconductor memory cards also exist and are used to store the encrypted code files. In addition to the encrypted code files, a portion or all of the data file decryption algorithm may also be stored on the blank media by the provider, preferably in the same non-copyable manner as the encrypted code.

This system of providing and using blank media does allow a user to make an unlimited number of copies, although only one at a time, which can be decrypted and played by any playback machine that is designed to read the decrypted identification code file that the provider has recorded on the media. Although this significantly reduces security of the data file contents, the content providers charge a fee for each blank recordable medium which is set to provide adequate compensation for the added copies that are possible.

Removable Code Card

Other approaches to the use of copies of encrypted data files in multiple utilization devices are possible. By at least replacing the memory portions 63 and 85 with a common memory on a removable credit card sized device, that is personal to a single user, this device can then be inserted into any utilization device capable of accepting this module. This will permit a user to play any content that has been encrypted with that user's personal identification code that is stored, in an encrypted form, in the memory on the removable device. Preferably, no two devices would be given the same identification code. One or more content decryption algorithms, in whole or in part, from different providers can also be stored in the device memory as a way of converting any utilization device in which the device is inserted into a general purpose player of content from multiple sources without the medium containing the content having to also carry the decryption algorithm. In order to make it more difficult to read portions of the device memory, it may be desirable to include the DSP and the DAC on the device as well in order to be able to encapsulate both the circuit chips and the lines connecting them in a manner to prevent user access to the contents of the memory and the unencrypted digital data.

As an alternative to providing an analog signal that is available to the user, the DSPs of the embodiments of Figures 1-3 can be configured to output a variable pulse width or variable repetition rate signal of the type currently used in class D audio amplifiers, in order to increase the level of copy protection. This alternative type of signal and its use are described below with respect to the embodiment of Figures 4-12.

A Further Secure Data Transmission and Use Embodiment

This personal code card (key card) concept is implemented somewhat differently in another system embodiment described with respect to Figures 4-12. Referring initially to Figures 4 and 5, a utilization device 101 is a portable, hand held audio player, as an example. Such a player is typically powered by batteries (not shown) that are contained within the player. Alternately, a utilization device for audio reproduction can be a component in a home stereo system, part of a car radio, a personal or portable computer, and other types of audio reproduction equipment. Of course, the various aspects of the present invention described with respect to the present embodiment are not limited in implementation to audio data transmission and reproduction, but rather apply to any type of data that is distributed and used in a similar way, such as video in the form of still pictures, movies or the like. But since audio reproduction, particularly music, through portable devices is likely to be a popular use, this is the example chosen to be described.

The player 101 contains the typical elements of human interface, including a display, 103, control knobs, buttons and/or sliders 105, and a loud speaker 107. A plug 109 for ear phones is also usually included, particularly if the loud speaker 107 is omitted. The content media is preferably a non-volatile semiconductor memory card 111, as currently commercially available, which stores digital data files of songs, albums or the like, in this example, and is removably inserted by hand into a socket of the device 101. Alternatively, other writeable non-volatile storage media may be employed, such as read/write compact discs (CDs). If the utilization device has its own large capacity mass memory, such as a personal or portable computer usually includes, such an internal memory may be used instead. A key card 115 includes a digital signal processor (DSP) and non-volatile memory to decrypt and decompress data files in the content memory, and is removably inserted into a socket 117 of the device 101. The non-volatile memory of the key card 115 stores, among other things, keys for encryption and decryption of data files stored in the content media 111. These keys are personal to the user of the utilization device 101 and, as described below, can be generated from a seed code that is included within the utilization device.

Also included in the audio player 101 is an optional communications jack 119 into which a plug 121 is removably inserted for downloading audio data files into the content media 111 through a communications circuit 123 such as a telephone line connected to the Internet. Alternate communication means may also be used, such as a local area network (LAN) or wireless communications. But the ability to download audio files into the memory card 111 need not always be provided in a utilization device. Such data files may be programmed into memory cards from a computer of the user that is connected to the Internet, a mass memory or Internet appliance or other network connection provided at music stores and the like, and any other source that is convenient for the user to access.

An example structure of the key card 115 is shown generally in Figure 5. One or more integrated circuit chips are surrounded by plastic surfaces, such as results from injection molding, to form an outer shell 125. Electrical contacts 127, connected with the circuit chip(s) within, are provided in some convenient form along one edge of the card 115 for making contact with conductors of the player socket 117 when inserted therein. Radiation shielding, such as layers of lead sheets, preferably surround the chip(s) within the card in order to minimize risks of its contents being viewed by x-ray techniques. The form factor, physical size and weight of the key card 115 are preferably chosen to allow easy transport, easy handling and robustness. For use with small hand held appliances, these requirements translate into a card as thin as practical and with a rectangular size approximating that of a postage stamp. The key card 115 is thus small enough to be easily carried by the user in a wallet, purse, and the like, in order that the user's audio cards, which may also be of the same small size, can be played on audio systems of others at various locations. A user may play music from his or her media though any music player utilization device by, at the same time, inserting his or her key card in the device along with the media. The transportability of the user's content, without compromising its security, is an advantage of the present implementation.

The utilization device 101, if a portable audio player, will usually be provided with only one socket 113 for a memory card 111 and only one socket 117 for the key card 115. Alternately, however, two or more sockets for simultaneously accepting two or more content media cards 111 may be provided. Since one hour or more of audio data is contemplated for storage on one such card 111, the insertion of multiple cards gives the user hours of uninterrupted music. Further, particularly if multiple content media card slots are provided, two or more sockets for simultaneously accepting two or more key cards 115 may be included in a utilization device, where the individual key cards contain different user data decryption keys. Audio data stored in different content media cards 111 by encryption with different user keys can then be easily played in succession without having to replace the key card 115 when different content media cards are accessed. Although provision for multiple key cards may not be made in portable audio players, which are usually used by one person, particularly one person at a time, this feature has a likely application to players for home stereo systems, car radios, and the like, where two or more users may come together to share their music that has been recorded on their different content media cards with their different personal encryption keys.

The schematic diagram of Figure 6 shows the primary electronic blocks of the utilization device 101, some of which have already been described. Central to the device is a control system 129 that will usually include a micro-processor, various logical circuits, a read-only-memory 131 and potentially other memory. The system control 129 interfaces to, and provides communication between, the content media 111, the user interface display 103, controls 105, the key card 115 and an optional communications module 133. The key card 115 includes an integrated circuit DSP chip 135 which processes data read from the content media 111 through the system control 129, and provides decompressed and decrypted content to a content processing block 137. In the example of an audio player, the content processing block 137 includes audio circuits for driving the loudspeaker 107 and/or ear phones 139 when plugged into the socket 109.

The DSP chip 135 in the key card includes an area 141 with processing circuitry, an area 143 of static random-access memory (SRAM), and an area 145 containing a read-only-memory (ROM). The ROM 145 is permanently programmed as part of the manufacturing process with certain files, including a boot file that the DSP circuitry first accesses in response to being initialized. An electrically re-programmable, non-volatile memory147, which is a flash ROM, is also preferably included on the same chip but may alternatively be formed on a separate chip electrically connected with the

DSP chip 135 and also sealed within the key card. The resulting key card is more secure when the flash ROM is on the DSP chip, since there are no wire connections that someone can undesirably access if the physical impediments presented by the structure of the card 115 are overcome. However, since flash ROM is formed by different technology than the rest of the chip 135, the combination often requires compromises to be made that are not optimal and can be expensive to make. Therefore, a separate flash ROM chip is often used. In either case, the integrated circuit chip(s) and the wires leading to them are physically encapsulated by a material that, when an attempt to remove it is made, will damage or destroy the chip(s) to prevent someone being able to access electrical connection points or closely inspect them to learn the values of encryption keys and other valuable information that could compromise data security.

Figure 7 itemizes, in a specific operating example, the software that is contained on one of the ROMs 145 or 147 of the DSP chip 135. A boot file 151 is stored on the ROM 145 that is not re-programmable. Key generation software 153, which allows the generation of a public key 155 and a private key 157, is preferably stored in the ROM 145, while the resulting keys are written into the flash ROM 147. Note that the key generation software 153 can be omitted and the public key 155 and a private key 157 pair can be programmed individually on each chip during the manufacturing process in a one time programmable ROM. This is equivalent to storing the resulting keys in the ROM 145. Decryption software 159 may be stored in either ROM, the security of storage in the ROM 145 being better but storage in the flash ROM 147 allowing the software to be updated. Although not preferable for security reasons, a portion or all of the decryption software may be sent by the content provider along with the content, rather than being stored in the key card, thus allowing each content provider to use different encryption/decryption algorithms, at least in part. Finally, either ROM can store the firmware 161 that operates the DSP to process the encrypted and compressed data content stored on the content media 111, depending upon whether it is likely that this firmware would be updated after manufacture.

The diagram of Figure 8 shows a process for the generation of public and private keys. In a first method, a password "seed" number is stored in the ROM 131 (Figure 6) of the system control block 129 of the utilization device. It is written there, in a manner that does not allow it to be read by the user, by the utilization device manufacturer. Alternatively, the seed can be internally created by an algorithmic process executed on the DSP within the key card, when the keycard is powered up for the first time, and stored in the DSP flash ROM 147. The key generation software 153, stored on the key card, takes the seed 163 from the utilization device ROM 163, in which it is inserted, or the DSP Flash ROM 147 in which it is stored, and generates a key pair: a public key 155 and a private key 157, which are then stored in the DSP flash ROM 147. As is described further below, the public key is readable from the flash ROM 147 to send to a content provider for use in encrypting the music or other content that the user orders. The private key, which is used by the DSP in the utilization device to decrypt that data, is not readable from outside of the key card. Thus, the software 153 generates the pair of keys to have that relationship. Such public/private key generation software is currently used for encryption/decryption of data files sent over the Internet but not in this manner. A key card with these keys is used each time that content is written by the utilization device onto its content media 111, wherein the public key is accessed, and each time that content stored on the media 111 is being played, wherein the unknown private key is read and used by the DSP internally within the key card.

Each seed stored by the utilization device manufacturer or internally created by an algorithmic process executed on the DSP within the key card, may be unique, not appearing on any other device. However, it is preferred that a significant number, such as ten-thousand out of a million seeds are the same so that there will be an equal number of the same public/private key pairs generated by the software 153. Alternatively, software 153 can produce unique private keys from a common seed which are associated with the same public key, thus causing a one-to-many public-to-private key relationship. Both of these approaches afford a measure of privacy to the user since the content provider cannot then identify the user from the public key alone.

The public key 155 may also be stored on blank content media 165 by use of the key generation software 153. This then allows the user to have audio data written onto the media 165 by some device other than the utilization device containing the seed from which the public key was generated by the software 153. If a music store, for instance, provides equipment to purchase encrypted music data files in the manner being described herein, the media 165 is inserted into a receptacle of the equipment which then reads the public key for use in encrypting the content data that is written by the equipment onto the media 165 in encrypted form. The content can then be retrieved from the media 165 when inserted into a utilization device into which a key card is also inserted that contains the private key that is paired with the public key used to encrypt the content.

An advantage of using the public/private key pairs is that the public key need not be stored or transmitted in an encrypted form, although it may be for some added degree of security, since it is not the key that is used to decrypt the content data. The private key, which is used to decrypt content data, is not known or accessible to the user. This provides a significant added degree of security to the system. Since it is not critical that a user's public key be kept secret, the user may send it to the provider in other ways than through the utilization device or from content media upon which it is stored. For example, it could be entered though a computer key board or a keypad on music store dispensing equipment. However, because of its length, it is usually preferable for the user to avoid having to manually enter the public key.

Referring to Figure 9, software components that are desirably stored in the DSP SRAM 143 are identified. Although already stored in ROM, the private key and content decryption software are copied into the SRAM since data can be read much faster from this type of memory, as is well known, during the very fast processing of the content data that must be performed by the DSP. The other software identified in Figure 9 is transferred from the content media 111 prior to playing the audio content, in a specific example being described, having been stored on that media by the content provider along with the audio content. Software 167 is used by the DSP to decompress the compressed audio content stored by the provider on the media 111. Alternatively, all or part of the data decompression software may be stored on the flash ROM 147 of the key card and then transferred into the DSP SRAM 143 as part of an initialization routine.

All or part of the content manipulation software 169 is optionally included by the content provider with the content and, if so, is used by the DSP 135 to post process the decrypted and decompressed data file. In the music example, the software 169 can allow the user to perform functions like adjusting the apparent amount of echo in the room in which the music was recorded, multi-channel multiplexing, equalization and other currently implemented audio functions. Subroutines provided by the content provider that make up the software 169 are inserted, at the option and under the control of the user, into the DSP firmware 161 so that such functions are provided. Alternatively, all or part of the content manipulation software may be stored in the DSP firmware 161 at the time of manufacture to provide such functions.

Content rights software 171 is also optionally used by the content provider to place limits on the use of the data content. This software also contains sub-routines that are inserted into the DSP firmware 161 when processing a data file. The content provider can use these sub-routines to do things like limit the number of copies of the content stored on the media 111 that can be made by the user, disable the playing of certain content after a certain date, which allows further revenue to be obtained by the content provider in order for the user to have the ability to play the data content after that date, and similar matters.

Figure 10 illustrates an example of the structure of a data content file sent by the content provider for storage on the user's content media. A primary component 173 is the data of the music or other content that has been compressed and encrypted. Decompression software 167', content manipulation code 169' and content rights code 171', corresponding to respective software 167, 169 and 171, are also included, in this specific example. A header 175 contains an inventory of the files included in the transmission and characteristics of components 167', 169' and 171'.

Referring to Figure 11, a flow chart of an example method is described for obtaining music or other content from a content provider and storing it on a user's content media. In a step 177, the user establishes a communication link between the content provider computer and the users content memory card or other media. This can be done either through the utilization device 101 or by connecting a blank card, with the user's public key stored on it, to content provider equipment at a music store or the like. A next step 179 provides user information to the content provider of an account with that provider for billing and verifies that there is an acceptable credit arrangement between the content provider and user. If the utilization device 101 is being used to obtain the content, this information can be sent by the user by appropriate manipulation of the its controls, or, if a blank card is inserted into content provider equipment, this information can be entered by the user directly into the equipment. Similarly, as indicated by a next step 181, the user sends an order for specific pieces of music or other content either through the utilization device or by input directly to content dispensing equipment at a music store or the like.

After these preliminary steps, the user's public key is read by the content provider, as indicated by a step 183, either from the DSP flash ROM 147 of a key card inserted in the utilization device 101, if being used to obtain the content, or from a blank memory card or other media 111, if being written directly onto the card. The selections of music or other content requested by the user are then assembled, as shown by a step 185, along with any accompanying software necessary to be included in the content file to be sent as described with respect to Figure 10. In a next step 187, the ordered music or other content data is then compressed and encrypted with the user's public key that was read by the content provider in the step 183. Some or all of the other software being sent at the same time, such as the software 167', 169' and 171', may optionally also be encrypted in the same way, but preferably not for these specific software and code examples since security of them by themselves is not of high concern. The header 175 (Figure 10) is also prepared in the step 187 (Figure 11) from information of the components of the content file being assembled. The header can contain a description and data of each piece of music contained within the content data 173, for example, plus information of the other software and code included. In a step 189, that assembled content data file is sent to the user and stored on the user's memory card or other content media, either through the utilization device 101 or directly by insertion into content provider equipment.

The content data file of Figure 10 is then available to the user for playing the purchased music through the utilization device 101. Referring to Figure 12, an example operation of the utilization device 101 is shown for doing so. In a first step 193, the boot file of the ROM 145 is read by the DSP. The boot file provides an instruction of where the DSP should go next. In a step 195, the DSP goes to its ROM and reads the files 157 and 159 (Figure 7) into its SRAM 143. The DSP also reads, in a step 197, the headers from the content data file(s) on the media to determine what items of music or other data are contained within it and the characteristics of any other software 167', 169' and 171' included with the content. The user, in a step 199, then selects an item of music, or multiple items of music, within the content file for play. For the selected content file, the DSP then compares the information in the header 175 of the accompanying software 167', 169' and 171' with that of any such software already in the DSP SRAM 143 as respective items 167, 169 and 171 (Figure 9). If any of these items are not in the SRAM, or if any one is not the same version as that provided with the content file being accessed, then the software that came with the content file is written into the SRAM 143.

The DSP then operates according to its firmware 161, the private key 157' and the software 159', 167, 169 and 171 to process the selected portion(s) of the content data 173, as indicated by a step 203. The result of this processing is audio or other data that is available for listening or other use by the user. In order to do so, however, this data is sent, in a step 205, to an audio or other content processor 137, whose output is in a form to drive a loud speaker or other user content interface device 107.

In the audio example, a digital-to-analog converter (DAC) can be used in a manner similar to the embodiments of Figures 2 and 3 to convert a standard digital sound output of the DSP 135 (Figure 6) into analog audio signals that can be amplified by the processor 137 sufficiently to drive the loud speaker 107 and/or ear phones 139. If such a DAC is used, it is encapsulated as part of the key card 115 in order to prevent unencrypted binary data being present at the output of the key card in a standard format that can be recorded by available digital recorders or easily sent over the Internet. Although content providers may be satisfied when a digital signal of low sample rate and resolution can be accessed by the user, better security is provided if no reasonable quality digital signal is accessible. And even when a DAC is included as part of the key card 115, its output is likely a reasonably high quality analog signal that an unauthorized copier can either record directly on an analog recorder or re-digitize and then either record digitally or send over the Internet. There remains some security advantage to the analog output, rather than the digital one, since the audio quality of an analog or re-digitized recording will likely not be as high as the audio content file would allow.

It is preferable, however, to cause the DSP 135 to output the audio or other content signal in a format other than a standard one that can be plugged directly into a recorder, sent over the Internet or otherwise easily used in an unauthorized manner. This may be accomplished by using techniques of a known class D type amplifier, where single bit pulses of varying width or repetition rate are generated from a sound signal and input to power circuits that efficiently drive loud speakers. The nature of the variable pulse widths or variable repetition rate depends upon the resistive and capacitive characteristics of the drive circuits and the loud speakers or ear phones being driven. The speakers are effectively turned on and off by such pulses after integration by a network including the drive circuits and the speakers themselves. It has been recognized that the class D technique can be used to advantage in the audio security system being described since a particular implementation provides no standard digital or analog signal after the DSP.

Therefore, the DSP 135 (Figure 6), through its firmware 161 (Figure 7), is caused to output the variable width or variable repetition rate pulses characteristic of a class D amplifier. This is the first signal that is accessible to the user from the DSP chip 135. It drives a class D power stage that is provided within the processing block 137, and then the loud speaker 107 or ear phones 139. The signal throughout the drive circuits, and even that applied to the loud speaker or ear phones, is a series of variable width pulses or repetition rate. A user cannot directly record such a signal with available equipment or transmit it over the Internet. Additional non-conventional circuitry would be necessary to convert the pulse width modulated signal into such a standard format with acceptable quality.

Further, since the drive circuits and loud speaker are non-linear devices, the pulse width or pulse repetition rate modulation is also made non-linear in a complementary manner, so the pulse stream output of the DSP 135, as well as the pulses in the drive circuits and those applied to the loud speaker and ear phones, can be of little use by themselves. Much sophistication would be necessary to be able to reformat the pulse width or pulse repetition rate modulated signal into something that is useful to record or send over the Internet, and then the quality would most likely be reduced because of the non-linearity. Another advantage of applying the Class D amplifier approach here is that the quality of the signal outputted by the DSP 135 need not be intentionally degraded to reduce its value to potential copiers. It is made to be as good as it can be made from the audio content file provided, without any significant risk that the high quality variable pulse width signal can be appropriated in another form with the same high quality.

The techniques and systems of this embodiment provide a significant amount of security of the data content being sent to a user. The content is not stored without encryption anywhere during transmission, or during storage and use. Use of the public/private key system of encryption and decryption of the content data makes it extremely difficult to determine the user's private key for decryption since it resides only on the encapsulated key card and preferably only within the non-volatile memory of the DSP chip. An unencrypted digital signal is never generated, except possibly on circuits within a single chip DSP that are not, as a practical matter, accessible by a user.

Even though a high level of security is provided, the user is given a great deal of flexibility on how it is used. The key card allows a user to play the content stored on a library of content media on any reproduction device. The ability to make duplicate keys allows the user to share his or her own library of content with family and friends. If utilization device manufacturers store the same seed in a number of devices, the user is then provided some privacy from inquiries of content providers of information in the user's computer or on content media, since many will have the same seed and resulting readable public key. Although these user features diminish the rights of the content providers, it is not very significant when compared to the increased use of the described content delivery methods that will result when the user is able to fully use the content as is now possible with other forms of the same content. That is, if music stored on memory cards may be played as easily and with the same flexibility as compact disks are now played, users will readily accept electronic delivery of music, to the benefit of music content providers.

Referring to Figure 13, use of the system embodiment described above with respect to Figures 4-12 is illustrated in a different manner. A provider of content, such as music, has a large database 301 from which certain content files, such as individual songs or performances, are selected for encryption 303. Files may be chosen, for example, by the end user designating them from a listing kept by the content provider and then paying for the right to download them. These selected files are encrypted with a public key 305 of the end user that is stored in a non-volatile memory of his or her sealed module 307. The module 307 structurally corresponds to the key card 115 that has been described with respect to Figure 6, and is illustrated in Figure 13 by the functions that it performs. The user's public key 305 is given to the content provider by some appropriate means such as being sent over the Internet. The selected content titles are then encrypted by the content provider with that public key. The encrypted files are then transmitted back to the end user by some appropriate means such as over the Internet. The user then stores the encrypted files on some suitable storage medium 309, such as a flash ROM card or Compact Disc.. Usually at some later time, that encrypted content is read from the storage medium 309 and subjected to decryption 311 by the user's stored private key 313. Decrypted content 315 is then available for use. If music, the content 315 is applied to an audio reproduction system.

Transcryption of Secure Data Files and Further Transmission and Use Embodiments

A technique for allowing a controlled transfer of the encrypted data files from one user to another, in a manner by which the second user can play or otherwise use their content, is illustrated by Figure 14. Data files on a first user's storage medium 317 are processed by a sealed transcryptor module 319 and then stored on a second user's storage medium 321. The module 319 uses a private key 323 of the first user, who has initially acquired the files on the storage medium 317 in a form encrypted by his or her public key, to decrypt (325) at least selected content files. This decrypted content is then encrypted (327) with the second user's public key 329, preferably supplied by the second user's sealed key card module 331. The transcryptor module 319 may be the key card module of the first user, with a connection added to receive the second users public key 329 from a similar key card module of the second user. It is highly preferable to perform the re-encryption function 327 within the same sealed module as the decryption in order to avoid making the decrypted content accessible to the user. The second user can then decrypt the content on the storage medium 321 by use of his or her private key that is stored within the second user's key card module.

As part of the decryption process 325, it is desirable to read the rights code 171' (Figure 10) for each content file, if included, in order to determine whether permission for such copying was given by the content provider when the content files were initially acquired. In order to control whether a content file can be copied, and, if so, to designate the number of times that copying is to be permitted, the content provider may designate that information in the rights code portion 171' of the individual content data files. If only a specified number of copies of a content data file is permitted, the encryption processing 327 then preferably rewrites its rights code 171' to indicate that one less copy may be made in the future. After all of the specified number of copies of a file have been made, the decryption processing 325 will, in response to reading the rights code 171', not permit any further copying. The number of copies that are allowed, if any, is a function of the price paid to the content provider for transfer of the file to the first user.

Alternatively, the rights code 171' of a data file may specify that any copy made of its music or other content will thereafter prevent the first user from accessing the file to play the music. Or, as a further alternative, such a lock out of the first user may occur after a specified number of copies are made. This allows the data file to be transferred but allows only one or the specified number of copies of it to exist. As an alternative to storing the rights codes as part of the respective content files, they may be stored within the non-volatile memory of the user's key card.

The ability of a music purchaser, for example, to transfer music files, or copies thereof, to friends and family may have to be permitted, especially in the case of music, by content providers if distribution of music in a secure manner is to be accepted by the public. Exercise of control by the content provider, as a function of how much was paid for the initial data file, is then desired by the content providers. In addition, in order for content providers to enable retail stores or others to distribute their music or other content to the end user, a method of transferring the content through such a middle party must be done with security.

A disadvantage of the transcryption technique described with respect to Figure 14, however, is that the entire content of the a data file needs to first be decrypted with one key and then re-encrypted with a second key. This can require a significant amount of processing for large files and/or if many such files are being transferred at one time. Therefore, a modified content data file distribution technique shown in Figure 15 has been devised. This method also provides advantages in the distribution and use of content data files, in addition to making secure transfers of them easier. The principle implemented is to encrypt each data file with a unique title key generated and maintained by the content provider, and then encrypt and decrypt the title key with the user's public and private keys in the same manner as described above for data files. But, in this case, the content data files are not encrypted or decrypted with the users keys.

Data files of a content provider's database 335, illustrated in Figure 15, are individually encrypted (337) with unique title keys that are stored in a database 339. The title keys are generated by the content provider, and each is keyed is linked to one of the content data files. A requested data file is communicated to an end user after encryption with its associated title key. In order for the end user to be able to decrypt the data file, the title key is encrypted (341) by the content provider with the user's public key that has been sent to the content provider by the user from his or her memory 342, and that encrypted title key then sent to the end user.

As shown in Figure 15, the data files encrypted with their associated individual title keys are sent in a convenient manner, such as over the Internet, to the user's storage medium. As before, the storage medium can be any convenient magnetic (such as a disk or tape), semiconductor (such as a non-volatile flash ROM card), optical (such as a Compact Disc) or other type of memory. The encrypted title keys may also be stored in the medium 343, as shown by the dashed lines, but there are advantages to storing them within the user's sealed storage and processing module 345. That is what is shown in Figure 15 in solid lines. The encrypted title keys are stored in a non-volatile memory 347. When a data file is desired by the end user, its associated encrypted title key is read out of the memory 347 for decryption (349) by the user's private key 351. The data file from the memory 343 is then decrypted (353) with the decrypted title key, and the decrypted content of the data file is outputted from the module 345, as indicated at 355. If the encrypted keys are stored in the memory 343 with the content data files, the decryption 349 receives the encrypted title keys from that memory instead of the memory 347.

The physically sealed module 345, shown in Figure 15 in terms of the functions it performs, is preferably constructed in the same manner as the key card 115 (Figure 4-9). One addition is a file in the flash ROM 147 of the encrypted title keys, corresponding to the memory 347 of Figure 15, if the encrypted title keys are stored in the key card itself. Another addition is decryption software to decrypt the title keys. The key card 115 operates differently when executing the technique of Figure 15 by decrypting the encrypted title keys, and then using the decrypted title keys to decrypt the content files. The decryption software 159 is then chosen to decrypt the content data files with the title keys instead of the user's private key as done in the previous embodiments. The module 345 should provide the same level of security as the key card 115, particularly by preventing access to digital signals that are not encrypted. The module 345 and delivery method illustrated in Figure 15 are advantageously used with digital files having audio, such as music, or video contents, but are not limited to use with data files having any particular content. When music content is being received, the content output 355 of the module 345 is preferably configured and used in the same manner as described for the key card 115 with respect to Figure 6.

When the encrypted title keys are stored in the module 345, they are preferably stored as separate files, an example structure of one such file being shown in Figure 16A. One encrypted title key 361 follows a header 363. The header includes an identification of, and preferably a link to, the encrypted data file within the storage medium 343 that is encrypted with that title key. The data file in the user's storage medium 343 can have the structure illustrated in Figure 10, with the header 175 also containing some link to its associated encrypted title key file within the module 345. Alternatively, if the encrypted title keys are stored on the user's storage medium 343, as indicated by the dashed path lines of Figure 15, each is preferably included as part of the same file as the data that has been encrypted with that title key, as illustrated in Figure 16B. The data file of Figure 16B is similar to that of Figure 10, a primary difference being the inclusion of a title key 365 with which the content data 173' is encrypted, the title key 365 having itself been encrypted with the user's public key.

The encrypted data files on the storage medium 343 (Figure 15) are now much easier to transfer than in the case described with respect to Figure 14. As illustrated in Figure 17, the encrypted content data files on a storage medium 371 of one user are transferred directly to a storage medium 373 of another user. Since each data file is encrypted with a title key that is independent of the users, no decryption and subsequent encryption of the data files are required when transferring them from the storage medium of one user to that of another user. Rather, this is performed only on the title keys that are associated with the transferred data files. Encrypted title keys 375 of user 1 that are stored in a memory of a sealed transcryptor 377 are decrypted (379) with a private key 381 of user 1 that is also stored in a memory of the transcryptor 377. The decrypted title keys are then encrypted (383) with the public key of user 2 that is stored in a memory 385 of a key card 387 of user 2. The encrypted title keys are then stored in flash ROM 382 of the module 387 of user 2. User 2 can then decrypt the data files transferred to his or her storage medium 373 by inserting the medium 373 and the key card 387 into an audio player, for example, as previously described.

The transcryption technique illustrated in Figure 17 thus minimizes the amount of data that must be decrypted by a key personal to user 1 and then again encrypted by a key personal to user 2. Of course, there is likely some input from the storage medium 371 to the decryption process 379 that identifies the data files being transferred from one storage medium to the other, so that the corresponding encrypted title keys are accessed from the memory 375 and transferred as well. This can be important if user 1 has a large number of stored encrypted title keys when only a few are to be transferred. Since the individual encrypted title key files (Figure 16A) are small, a large number of them can easily be stored on a user's personal key card.

The transcryptor 377 can be a key card of user 1, with its DSP programmed to perform the decryption and encryption processes 379 and 383. The title key output of the card 377 is encrypted. No access to a decrypted title key is provided since that is present only within the sealed module 377. Some connector box (not shown) is conveniently provided for interconnecting the key cards of the two users in order to allow the transfer of the described key files between them.

As an alternative to storing the encrypted title keys in the users' key cards, they may be stored as part of the content data files themselves, as previously described. In this case, the encrypted title keys are read from the storage medium 371 for the decryption 379, as indicated by the dashed path of Figure 17. Similarly, the encryption 383 then writes the newly encrypted title key as part of the data file stored on the copy storage medium 373, the file structure following that of Figure 16B where the newly encrypted title key replaces the original encrypted title key from the storage medium 371. The private key of user 2 can then be used to decrypt the encrypted title key newly stored on copy storage medium 373, which can in turn be used to decrypt the content 173" of the file in the storage medium 373, while the private key of user 1 cannot. Alternatively, the original encrypted title key may be retained while the newly encrypted title key is added to the data file, as illustrated in Figure 18, where both encrypted title keys 391 and 393 are included. This then allows the content of the data file to be retrieved from the storage medium 373 with use of the private keys of either user 1 or user 2.

To further increase the usability of such stored data files, particularly when the content is music, it is desirable to be able to play the content from two or more users' storage media in a single player. For example, if one user is hosting a party where music is being played from such data files on his or her player, it is often desired to play music on the same player from the content data files of one or more visitors who bring to the party both the content storage media and their personal key cards. One way to accomplish this is for the visitor to insert his or her key card into the host's player, along with the visitor's content medium, and then let the DSP within the visitor's card to do the processing to decrypt the visitor's music data files. Another way to accomplish this is illustrated in Figure 19, wherein the player is provided with a second key card slot to receive a visitor's key card as well as the host's key card 397. The DSP in the host's key card 397 accomplishes the content decryption while the visitors key card 395 functions to change the encryption of the title keys of the music files the visitor wants to play from the visitor's key to that of the host. The host key card can then decrypt the title keys, and thus use the decrypted title keys to decrypt the content files.

Referring to Figure 19, this title key encryption translation is illustrated. The visitor's stored encrypted title keys 399 are decrypted (401) within the visitor's module 395 by use of a stored visitor private key 403. The decrypted title keys are then re-encrypted (405) within the visitors module 395 with the host's public key 407 that is stored in the host's module 397. The newly encrypted title keys are then stored in a memory 409 of the host's module 397. They are then decrypted (411) by the host's private key 413, and the decrypted title keys used to decrypt (415) their corresponding music content data files stored on the visitor's content medium 417. The result is an audio output 419, which may be one of the types of signals previously discussed as being outputted from the key card 115 of the audio system of Figure 6, and utilized in the same manner as there described.

The use of encryption by content providers of content data files with title keys, which are then encrypted by the recipient's key and transmitted along with the encrypted contents or separately from the encrypted contents, also has advantages in the electronic distribution of music, or other data, to end users through one or more intermediaries in a chain of distribution. Such an intermediary can include a distributor, and, if a wholesale distributor, also a retail store. The content provider places its encrypted content files and title keys into this chain of distribution by transferring them to the first intermediary over a communication network such as the Internet or, alternatively, on a physical media such as a computer disk or tape, that is physically delivered. The end user retail customer receives the encrypted content files and title keys from the last intermediary in the distribution chain, either over a communication network such as the Internet or by connecting his or her storage medium to a distribution device such as a kiosk. A kiosk can be operated by a retail store in its facilities, for example, or as a stand-alone unit positioned in a public place. The content provider may distribute given content files through two or more such distribution chains.

Figure 20 illustrates one such distribution system, as an example, where a single intermediary distributor 425 is positioned between the content provider and the end user customer. The functions performed by the content provider are the same as those previously described with respect to Figure 15, so are not repeated here, the same reference numbers being used on Figure 20 for elements that correspond to those of Figure 15. The primary difference is that the title keys are encrypted (341) for transmission by the content provider with a public key 427 provided by the intermediary instead of that of the end user. The encrypted title keys are then stored by the intermediary in a mass storage system 491. Similarly, the encrypted content files are stored by a mass storage system 493, which may be common with the storage 491.

The end user customer then obtains the encrypted content data files and title keys from the intermediary. The user's content media and module shown in Figure 20 are the same as those shown in Figure 15, with the same reference numbers used to identify corresponding components and functions. The previous description of those elements is not repeated here. When the end user wants to obtain one or more content data files, the intermediary 425 identifies the corresponding title keys in its memory 491 and decrypts (495) the title keys by use of its private key 497. The title keys are then encrypted (499) with the public key 342 sent by the end user. The encrypted title keys are then loaded into non-volatile storage 347 of the user's module 345. At the same time, the desired encrypted content data files are loaded into the user's content medium 343. The end user is then able to decrypt and play the content files in a manner previously described.

A physical form of the intermediary 425 can be a kiosk, where the end user inserts his or her key card module and storage medium into the kiosk to provide the user's public key and receive the encrypted data and title keys. The kiosk also will include some way for the end user customer to pay for the data files, by credit card, cash or the like, before the transfer takes place.

As a modification to the distribution method illustrated in Figure 20, the encrypted content 493 is distributed by the retail store or other intermediary as illustrated. But rather than such an intermediary also distributing the encrypted title keys, in order to limit the number of entities having access to the encrypted title keys, the content provider or some other intermediary can provide them instead. For example, in the case of a large record store chain, each store can provide the content while a head office of the store chain, or a few regional distribution centers, can provide the encrypted title keys that go with the content. In that case, the end user customer transmits his or her public key to such a central location, which is used to encrypt the title keys for the content purchased at the retail store and send them directly to the customer. Kiosks in retail stores can operate in this manner, for example, where the local retail stores provide the encrypted music files but do not posses the encrypted title keys. The customer conveniently obtains them over a communications system from a central location while the customer is still in the store.

As previously emphasized, the end user's content storage media may take a number of different forms. Although a small flash ROM card is a very convenient storage medium, particularly when used with a portable audio device, a recordable Compact Disc also may be used. Such a Compact Disc 501 is illustrated in Figure 21. The encrypted content files are stored in an area 503 in the same manner as music or other data is currently optically recorded on Compact Discs. The title keys which have been encrypted to the owner's public key are conveniently written on a label 505 attached at a center of the disc 501. These encrypted title keys may be encoded in the form of a bar code or the like. A standard Compact Disc label maker can be configured to print the encrypted title keys on the label, which can be affixed to the Compact Disc using mechanical means or by the end user, while a standard recordable Compact Disc writer can be used to optically write the ordered encrypted data files to the disc using a file structure like that shown in Figure 10. Such a disc is played back by the end user through a Compact Disc player of a standard type that is modified to additionally optically read the encrypted title keys printed on the label.

Alternatively, the Compact Disc writer can write both the ordered encrypted data files to the disc along with the encrypted title keys using data file structures shown in Figure 16B. Standard Compact Disc players, DVD players or CD-ROM equipped Personal Computers, with a digital output, can then be used in conjunction with an external module connected to this digital output, in which the user's key card is inserted, to listen to the acquired music content. The analog output from this module is connected to standard amplification and speaker means to effectuate the listening experience. An additional alternative, which uses the file structure of Figure 18, can also be used. The use of such a file structure results in a Compact Disc playable by two or more end user key cards. In this case, two or more user's key cards are made to be accessible to the kiosk producing the Compact Disc. In all of these three alternative embodiments, an end user's key card receives both types of encrypted files from the Compact Disc player for processing by its DSP to obtain the audio or other content.

Another way to use such CDs is to physically distribute pre-pressed CDs which can be "personalized" to a users public key at the time of purchase at a retail outlet. Each song of the music data pressed onto the CD is be encrypted to a separate title key, as before. This title key, and any associated rights code, are not included on the disc. Therefore the disc cannot be played by any player, without additional data. The record label (or record distributor, depending on how trusted the record distributor is) can send by electronic means (over the Internet, for example) to the retail record store, a database of CD song titles and associated encrypted title keys. These title keys are encrypted to the retail record store's transcryptor module's public key. At the time of purchase, the customer's key card module public key, the retailer's database of CD song titles and associated encrypted title keys and the store's transcryptor module's private key are used to transcrypt the particular song's title key to one which is encrypted to the customer's public key. (See Figure 20) The resulting transcrypted title key is then printed on an optically readable label which is affixed to the pre-pressed CD. To play this pre-pressed CD, with the affixed label in place, the customer places the disc into his or her's CD, DVD or personal computer CD-ROM player, or any player capable of reading the disc, and inserts his or her key card module into a module slot provided in the player. The encrypted song data, along with the personalized transcrypted title key read from the affixed label, is inputted into the customer's key card, where the key card's private key is used to first decrypt the title key and then the decrypted title key is used to decrypt the song data. All of this processing occurs within the sealed key card module, so there is no access to the decrypted compressed or decompressed digital data. Only an analog signal representative of this digital data is available to the end user for listening. Note, in this embodiment, that it is not necessary for the music data to be compressed. It can be carried on the CD (or DVD if desired) in non-compressed PCM form, at what ever data rate is appropriate for the desired music quality. This means that this use of transcryption can serve the secure distribution needs of standard CD, DVD Video and DVD Audio formats, as well as all compressed audio formats.

As an alternative to printing the encoded title keys on the disc label, they may be directly downloaded into the flash ROM embedded inside the customer's key card, which is used during the transcryption process anyway to provide the user's public key. The key card flash ROM can store many megabytes of data. If each encoded title key is composed of 1024 bits, for example, a key card can store the title keys for over seventy thousand songs in just 10 megabytes of flash ROM. This means that a single key card module can store the users digital rights and title keys for a collection very much larger than 70,000 songs, for flash ROM is currently available in capacities which exceed 256 megabytes. A special player, capable of reading a label affixed to the CD carrying the encrypted song, is not required. Since the right and keys are stored in the key card, a standard CD player, DVD player, or Personal Computer can be used, with an external module as previously described.

It should be noted that in those cases where it is undesirable or impractical for encrypted song title keys and/or digital rights files to be in the possession of the distributor or retailer, both of these files can be personalized and provided directly to the consumer by the content owner, either at the check out counter of the retail store or at the user's home over the Internet. In the retail store, or at home, the users keycard is be inserted into equipment connected to a record labels title key and rights database and the user's public key is used directly in the process of personalized title key and rights preparation. A standard personal computer adapted to accept the user keycard through the use of an add-on module to the USB port, for example, can be used. The intermediate steps of first transferring the title key to the retailers public key and then transcrypting the title key from the retailers public key to the user's public key is not required

Another use of the transcryption process described above is to sell a disc, with many song titles on it, but give the user the ability to play only the song titles to which he or she has acquired rights by an appropriate payment. A DVD can have a data storage capacity of 8.3 Gigabytes. A song is usually between 3 and 5 minutes in length. When compressed, acceptable reproduced music quality requires about 1 megabyte of storage per minute of music. Thus, a 5 minute song produces a 5 megabyte file. Being conservative, a disc which can hold 8.3 Gigabytes of data can therefore hold 1660 songs. This is a sufficient number of songs for the complete collection of music works from a very productive famous artist. Such a disc would be very costly, not from the standpoint of producing and replicating the disc, but from the standpoint of paying the artist for his or her entire collection of work. Since the masters of the songs of famous artists are all currently available, the cost of creating a disc with an artist's complete works is minimal. However, the royalty necessary to be paid to the artist for each song provided to the customer would be a very large sum. If a famous artist were to be compensated on the basis of the sale of the disc which contained his or her entire life's work, this disc would have to cost the customer many thousands of dollars.

But by using the transcryption techniques described above, the customer can be provided the rights to listen to only one or a few of the songs on the disc, and the customer need then only pay for the songs for which the right to listen has been obtained. These rights can be downloaded into the flash ROM of the customer's key card module, either at the checkout counter of the retail store where the disc is purchased or over the Internet after the disc has been purchased and brought to the customers home. The physical media with the entire collection of a famous artist can be sold for a few dollars, with payment for the rights to play each song provided at the time the customer wishes to enjoy the song. In this manner, the customer has to pay for the songs the customer likes and not pay for the songs to which he or she does not want to have access. Note that this method of song distribution provides instant access to the song. Since it does not require the lengthy and tedious download of the entire artist's collection itself (the customer already has the music data in his or her possession, for it resides on the DVD previously purchased), the time required for the customer to obtain access to the song he or she wants to hear is only related to the time required to transcrypt the title keys of the songs that the customer wants access to. This process requires only a matter of seconds. Although it need not be performed by the store in which the disc is purchased, each store can have a database with title keys encrypted to that store's public key, as well as the tools necessary to transcrypt selected ones of the title keys from an encryption to the store's public key to one that is encrypted to the customer's public key. This service can be provided in the store or over the Internet, which ever is more convenient for the customer.

Referring to Figure 22, an example of the foregoing, in one form, is illustrated. The customer's key card module 345 is the same as used in the transcryption process of Figure 20, as described with respect to Figure 15. But instead of a recordable storage medium on which the encrypted data files are stored by the user, the user purchases a disc or other storage medium 511 that contains many songs, in a large number of such data files, more than the user may wish to access at the time of original purchase. Since each data file, or each of a defined group of data files, on the media 511 is encoded with a unique title key, the customer may purchase the title keys, encoded to his or her public key, or all of the files, or groups of files, for which access in an unencrypted form is desired. This is done by the content provider, distributor, retail store, kiosk or other provider encrypting (513) the purchased title keys with the user's public key 342 as stored on his or her key card module 345. This can be done over the Internet after the medium 511 is purchased, at the store where the pre-recorded medium is purchased, either at the time of the purchase or later, or in some other manner.

Additional title keys can also be purchased at different times for a given disc or other medium.

Although the various aspects of the present invention have been described with respect to specific embodiments thereof, it will be understood that the invention is entitled to protection within the full scope of the appended claims.

IT IS CLAIMED:

1. A method of transferring digital data from a provider to a user, comprising:

the user sends an encryption code and it is received by the provider,

the provider encrypts the digital data with the received encryption code according to an encryption algorithm,

the provider sends the encrypted digital data and it is received by the user, and

the user decrypts the received encrypted digital data with a decryption code stored in an electronic memory of the user and a decryption algorithm.

2. The method of claim 1, wherein the encryption and decryption codes are the same, the encryption code is transferred from the user to the provider in an encrypted form, and the user has no access to the decryption code.

3. The method of claim 1, wherein the encryption and decryption codes are respectively different pairs of public and private keys, and the user has no access to the private key.

4. The method of any one of claims 1-3, wherein the digital data includes at least one content file.

5. The method of claim 4, wherein said at least one content file includes data of an analog audio or a video signal.

6. The method of any one of claims 1-3, wherein the digital data includes at least one title key without a content file, the method further comprising the provider encrypting at least one content file with said at least one title key, the provider sending the encrypted content file to the user, and the user decrypting the received content file with the decrypted at least one title key.

7. The method claim 5, wherein said at least one content file includes data of an analog audio or a video signal.

8. The method of any one of claims 1-3, wherein the user decrypts the received encrypted digital data without having access to the digital data in an unencrypted form.

9. The method claim 8, wherein said at least one content file includes data of an analog audio or a video signal.

10. The method of claim 4, wherein said at least one content file includes data of an analog audio signal, and the user decrypts the audio data into a sequence of pulses having a variable repetition rate that represents the analog signal.

11. The method of claim 4, wherein said at least one content file includes data of an analog audio signal, and the user decrypts the data into a sequence of pulses having variable widths that represents the analog signal.

12. The method of any one of claims 1-3, wherein the encryption code is transferred by the user to the provider and the encrypted digital data is sent by the provider to the user over the Internet.

13. The method of any one of claims 1-3, wherein the user stores the encryption and decryption codes in an electronic memory which is contained within a sealed card that is removably inserted into a device of the user that utilizes the digital data.

14. The method of claim 13, wherein the encrypted digital data received by the user is stored on memory media that is also removably inserted into the device of the user that utilizes the digital data.

15. The method of claim 13, wherein processing to decrypt the encrypted digital data is carried out by a processor within the sealed card.

16. The method of claim 15, wherein the processor outputs an analog signal from the sealed card.

17. The method of claim 15, wherein the processor outputs from the sealed card a series of pulses with varying widths representing an analog signal.

18. The method of claim 15, wherein the processor outputs from the sealed card a series of pulses having a varying repetition rate representing an analog signal.

19. The method of claim 4, wherein the provider additionally sends to the user, along with the encrypted digital data, software code that affects use of the digital data.

20. The method of claim 19, wherein the software code manipulates the digital data of said at least one content file after decryption in a manner that is selectable by the user.

21. The method of claim 19, wherein the software code designates an extent of rights of the user in said at least one content file.

22. The method according to claim 2, wherein the encryption code is transferred from the user to the provider over a communications network, and wherein the encrypted digital data and any portion of a decryption algorithm not possessed by the user is transferred from the provider to the user over the communications network.

23. A method of communication of a digital data file from a content provider to a user, comprising:

the user sends to the provider a unique identification code that has been encrypted by a code encryption algorithm to which the user does not have access, the provider decrypts the encrypted identification code by use of the code encryption algorithm and then encrypts the data file according to a data encryption algorithm with the decrypted identification code as a key,

the encrypted data file is then sent by the content provider to the user, and

the user then decrypts the encrypted data file by use of the key obtained by locally decrypting the encrypted identification code possessed by the user but without providing access of the user to either the identification code or the code decryption algorithm.

24. The method of claim 23, wherein the data file includes digital data of an analog signal, and the user converts the decrypted data file into the analog signal without having access to any unencrypted digital data of the file.

25. The method of claim 23, wherein the encrypted identification code is stored on a utilization device of the user from which it is sent to the provider.

26. The method of claim 23, wherein at least a portion of the data decryption algorithm is maintained by the user in a manner that is not accessible by the user and any additional portion of the data decryption algorithm is sent by the content provider along with the encrypted data file.

27. The method of claim 23, wherein the encrypted data file is sent to the user by the content provider over the Internet.

28. A method of communication of a digital data file from a content provider to a user, comprising:

the user generates public and private keys in a manner that the public key is accessible but the private key is not accessible,

the user sends the public key to the provider,

the provider encrypts the data file with the public key according to a data encryption algorithm,

the encrypted data file is then sent by the content provider to the user, and the user then decrypts the encrypted data file with a decryption algorithm that uses the private key.

29. The method of claim 28, wherein the public and private keys are stored in a memory within a sealed key card that is removably connectable with a user device that utilizes information contained in the digital data file.

30. The method of claim 29, wherein the user sends the public key from the key card memory to the provider.

31. The method of claim 29, wherein the received encrypted data file is decrypted by a processor contained within the sealed key card.

32. The method of claim 31, wherein the decrypted data is outputted from the sealed key card in a form other than binary code.

33. The method of claim 32, wherein the decrypted data is outputted from the sealed key card in a form of pulses having varying widths according to the digital data.

34. The method of claim 32, wherein the decrypted data is outputted from the sealed key card in a form of pulses having a varying repetition rate according to the digital data.

35. The method of any one of claims 29-32, wherein the encrypted data file sent to the user is stored in a memory that is removably connectable with a user device that utilizes information from the digital data file.

36. The method of claim 35, wherein said memory is a non-volatile semiconductor memory card.

37. The method of claim 28, wherein the public key is stored in a memory that is removably connectable with a user device that utilizes information from

the digital data file, and the user sends the public key from the memory to the provider and the encrypted data file sent to the user is stored in said memory.

38. The method of claim 37, wherein said memory is a non-volatile semiconductor memory card.

39. The method of any one of claims 28, 29 or 37, wherein the digital data file includes a digitized analog signal.

40. The method of claim 39, wherein the analog signal includes an audio music signal.

41. A method of communicating selected ones of a library of digital data files from a content provider to a user, comprising:

the provider maintains different title keys associated with individual ones of the digital data files,

the provider encrypts at least one of the library of data files with its associated title key,

the user sends an encryption key to the provider,

the provider encrypts said associated title key with the encryption key received from the user according to a data encryption algorithm,

the encrypted at least one of the library of data files and the encrypted associated title key are then sent by the content provider to the user,

the user then decrypts the encrypted associated title key with a decryption algorithm that uses a decryption key, and

the user then decrypts the encrypted at least one of the library of data files with the decrypted associated title key.

42. The method of claim 41, wherein the encryption and decryption keys are respectively different pairs of public and private keys, and the user has no access to the private key.

43. The method of claim 42, wherein the public and private keys are stored in a memory within a sealed key card that is removably connectable with a user device that utilizes information contained in said at least one of the library of data files.

44. The method of claim 43, wherein the received encrypted at least one of the library of data files and the received encrypted associated title key are both decrypted by a processor contained within the sealed key card.

45. The method of claim 44, wherein the decrypted data is outputted from the sealed key card in a form other than binary code.

46. The method of claim 45, wherein the decrypted data is outputted from the sealed key card in a form of pulses having varying widths according to the digital data.

47. The method of claim 45, wherein the decrypted data is outputted from the sealed key card in a form of pulses having a varying repetition rate according to the digital data.

48. The method of 41, wherein the encrypted at least one of the library of data files sent to the user is stored in a memory that is removably connectable with a user device that utilizes information from the digital data file.

49. The method of claim 48, wherein said memory is a non-volatile semiconductor memory card.

50. The method of claim 48, wherein said memory is an optical disk containing the encrypted at least one of the library of data files optically stored therein and the encrypted associated title key printed on a label provided in a center portion of the optical disk.

51. The method of any one of claims 41 - 44, wherein said at least one of the library of data files includes a digitized analog signal.

52. The method of claim 51, wherein the analog signal includes an audio music signal.

53. A method of transferring at least one data file from a first party to a second party, comprising:

providing said at least one data file in a form encrypted with an associated title key, and providing said associated title key in a form encrypted with a key of the first party,

decrypting the associated title key by use of the first party's key, and encrypting the associated title key with a different key of the second party, and

transferring both said at least one data file encrypted with the associated title key and the associated title key encrypted with the second party key.

54. The method of claim 53, wherein decrypting and encrypting of the associated title key are accomplished in a sealed module that includes a processor.

55. The method of claim 53, wherein the first party is a content provider and the second party is a retail store.

56. The method of claim 53, wherein the first party is a first individual user of the data file and the second party is second individual user of the data file.

57. The method of claim 53, wherein transferring additionally includes transferring the associated title key encrypted with the first party key.

58. The method of any one of claims 53 - 56, wherein the data file includes digital data of an audio analog signal of music.

59. A method of distributing music to end users, comprising:

physically transferring to an end user a storage medium containing a plurality of pieces of music in digital form that are individually encrypted to one of a plurality of title keys, and selling to the end user at least one of the plurality of title keys corresponding to at least one individual piece of music but less than all of said plurality of pieces of music on the storage medium, wherein the plurality of title keys sold to the end user are encrypted to an encryption key of the end user.

60. The method of claim 59, wherein the plurality of pieces of music are stored on an optical disk and the title keys encrypted to an encryption key of the end user are printed on a label forming part of the optical disk.

61. An electronic circuit key card removably connectable with a host system, the card comprising a digital signal processor adapted to receive an encrypted digital data file of an analog signal from the host and decrypt the digital data file by use of decryption software and a key therefore that are stored in a non-volatile memory on the circuit card, wherein the key is either specific to the individual circuit card or personal to a user of the card and is stored in a manner not readable by the user of the card.

62. The circuit card of claim 61, additionally comprising a digital-to-analog converter connected to receive the decrypted data file from the processor to retrieve the analog signal contained in the encrypted digital data file, said replica analog signal being an output of the circuit card.

63. The circuit card of claim 61, wherein the processor decrypts the digital data file in a manner to form a signal of pulses of varying width that represent the analog signal, said signal of pulses being an output of the circuit card.

64. The circuit card of claim 61, wherein the processor decrypts the digital data file in a manner to form a signal of pulses of varying repetition rate that represent the analog signal, said signal of pulses being an output of the circuit card.

65. The circuit card of claim 61, wherein decompression software is also stored in the non-volatile memory on the circuit card and used by the processor to decompress the digital data file.

66. The circuit card of claim 65, wherein software is also stored in the non-volatile memory on the circuit card to manipulate the received digital data in a manner to alter the analog signal decrypted therefrom.

67. The circuit card of claim 61, wherein the key is stored in a manner to not be readable by the user of the card by encrypting it.

68. The circuit card of claim 61, wherein the key is stored in a manner to not be readable by the user of the card by storing it in the non-volatile memory in a manner that the signal processor has access to it but does not allow the key to be read from outside of the card.

69. The electronic circuit card of any one of claims 61-65, wherein the processor and memory are encapsulated on the card in a manner to protect them and any circuits extending between them from being accessed by a user.

70. An audio player, comprising:

a case containing control and audio circuits that drive a listening device,

a connection to removably receive a data storage device that stores encrypted digital data files of audio signals, and

a connection to removably receive a sealed key card, wherein said key card includes:

a non-volatile memory containing a decryption key that is either specific to an individual player or personal to a user of the player and which is not readable by the user, and

a processor that receives an encrypted digital data file of an analog audio signal from the storage device and processes said data file including decrypting it by use of the decryption key stored in the non-volatile memory to generate a decrypted signal therefrom that is applied to the audio circuits.

71. The player according to claim 70, wherein at least a portion of decryption software is stored in the non-volatile memory for use by the processor to decrypt the digital data file.

72. The player according to claim 71, wherein at least a portion of data decompression software is stored in the non-volatile memory for use by the processor to decompress the digital data file.

73. The player according to claim 70, wherein the data storage device includes non-volatile semiconductor memory in the form of a card and the connection to removably receive the data storage device includes a memory card socket in the case into which the memory card is manually inserted.

74. The player according to claim 73, wherein the case includes a plurality of said memory card sockets, thereby to provide for simultaneous connection of a plurality of memory cards therein.

75. The player according to claim 74, wherein the connection to removably receive a sealed key card includes a plurality of key card sockets in the case into which a plurality of key cards may be simultaneously inserted.

76. The player according to claim 70, wherein the audio player is portable and powered by batteries contained within the case.

77. A method of creating and storing a pair of public and private keys, wherein the private key can decode a data file that has been encoded with the public key, comprising:

utilizing a sealed module having a processor and a memory interconnected with the processor,

storing software within the module memory for generating the pair of public and private keys,

causing the processor to execute the key generating software to generate the pair of public and private keys in response to a seed, and storing the generated public and private keys in a manner that the private key is not electrically accessible from outside the module.

78. The method of claim 77 in which the seed is generated within the sealed module.

79. The method of claim 77, additionally including loading, without user intervention, the seed into a memory of at least one module from a host system to which said at least one module is removably connected.

80. The method of claim 79, additionally including loading, without user intervention, the seed into the memories of a plurality of modules from a single host system to which the modules are removably connected.

81. The method of either one of claims 79 or 80, wherein the seed is loaded from a memory within the host system.

82. The method of claim 77, wherein the key generating software generates, from a single seed, a plurality of private keys for a single public key.

83. A storage disc, comprising:

a first circular region on which a plurality of content data items are optically recorded in a form individually encrypted with a corresponding one of a plurality of title keys, and

a second circular region surrounded by the first circular region and containing printed thereon at least one of said plurality of title keys that is encrypted with a user key and which corresponds to at least one of the plurality of content items optically recorded on the first region.

84. The storage disk of claim 83, wherein the number of encrypted title keys printed in the first region is less than the number of said plurality of content data items optically recorded on the first region, thereby leaving at least one of the

plurality of content data items without a corresponding encrypted title key printed in the second region.

85. The storage disk of claim 83, wherein each of a plurality of title keys printed on the second region are encrypted with a common user key.

86. A storage disc, comprising:

a circular region on which a plurality of content data items are optically recorded in a form individually encrypted with a corresponding one of a plurality of title keys, and

at least one of said plurality of title keys that is encrypted with a user key and which corresponds to at least one of the plurality of content items optically recorded on the circular region is stored in a separate sealed module.

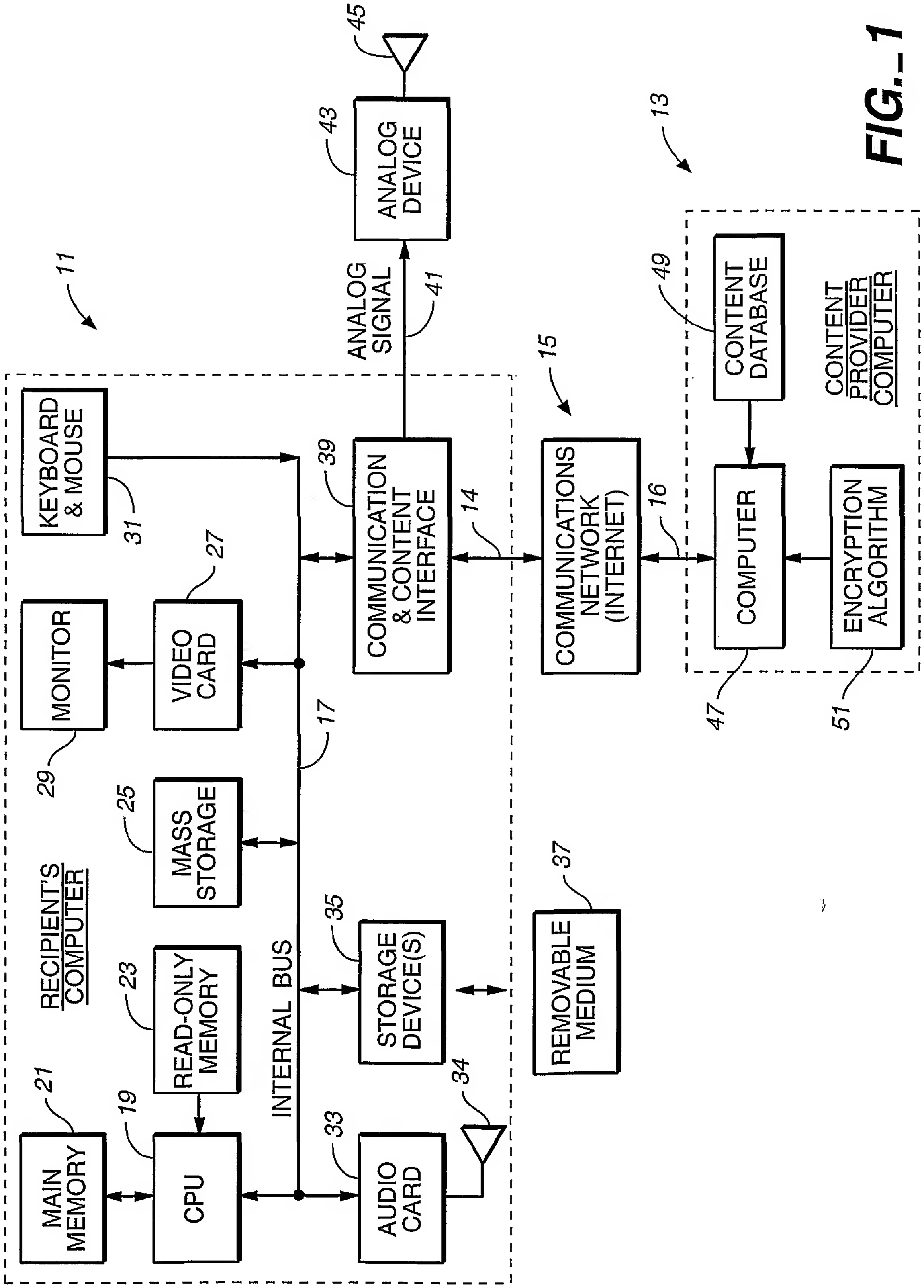

11
RECIPIENT'S COMPUTER
MAIN MEMORY
21
CPU
19
READ-ONLY MEMORY
23
MASS STORAGE
25
MONITOR
29
VIDEO CARD
27
KEYBOARD & MOUSE
31
INTERNAL BUS
17
AUDIO CARD
33
34
STORAGE DEVICE(S)
35
REMOVABLE MEDIUM
37
COMMUNICATION & CONTENT INTERFACE
39
14
ANALOG SIGNAL
41
ANALOG DEVICE
43
45
COMMUNICATIONS NETWORK (INTERNET)
15
16
13
CONTENT PROVIDER COMPUTER
CONTENT DATABASE
49
COMPUTER
47
ENCRYPTION ALGORITHM
51

FIG._1

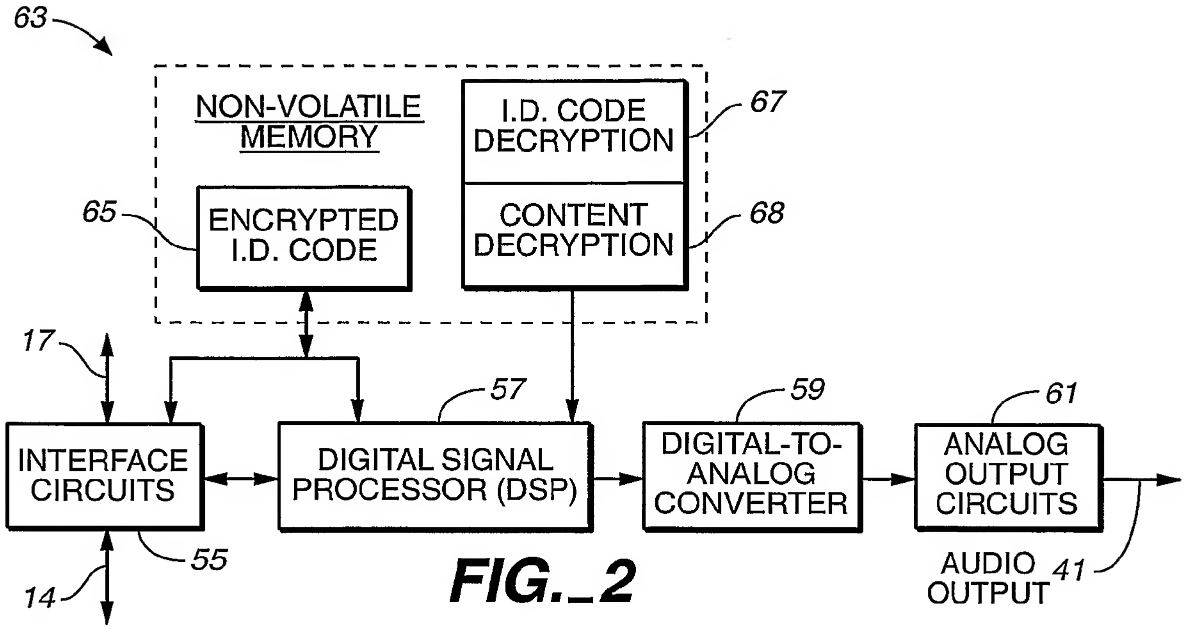

63
NON-VOLATILE MEMORY
I.D. CODE DECRYPTION
67
65
ENCRYPTED I.D. CODE
CONTENT DECRYPTION
68
17
57
59
61
INTERFACE CIRCUITS
DIGITAL SIGNAL PROCESSOR (DSP)
DIGITAL-TO-ANALOG CONVERTER
ANALOG OUTPUT CIRCUITS
55
14
AUDIO OUTPUT
41

FIG._2

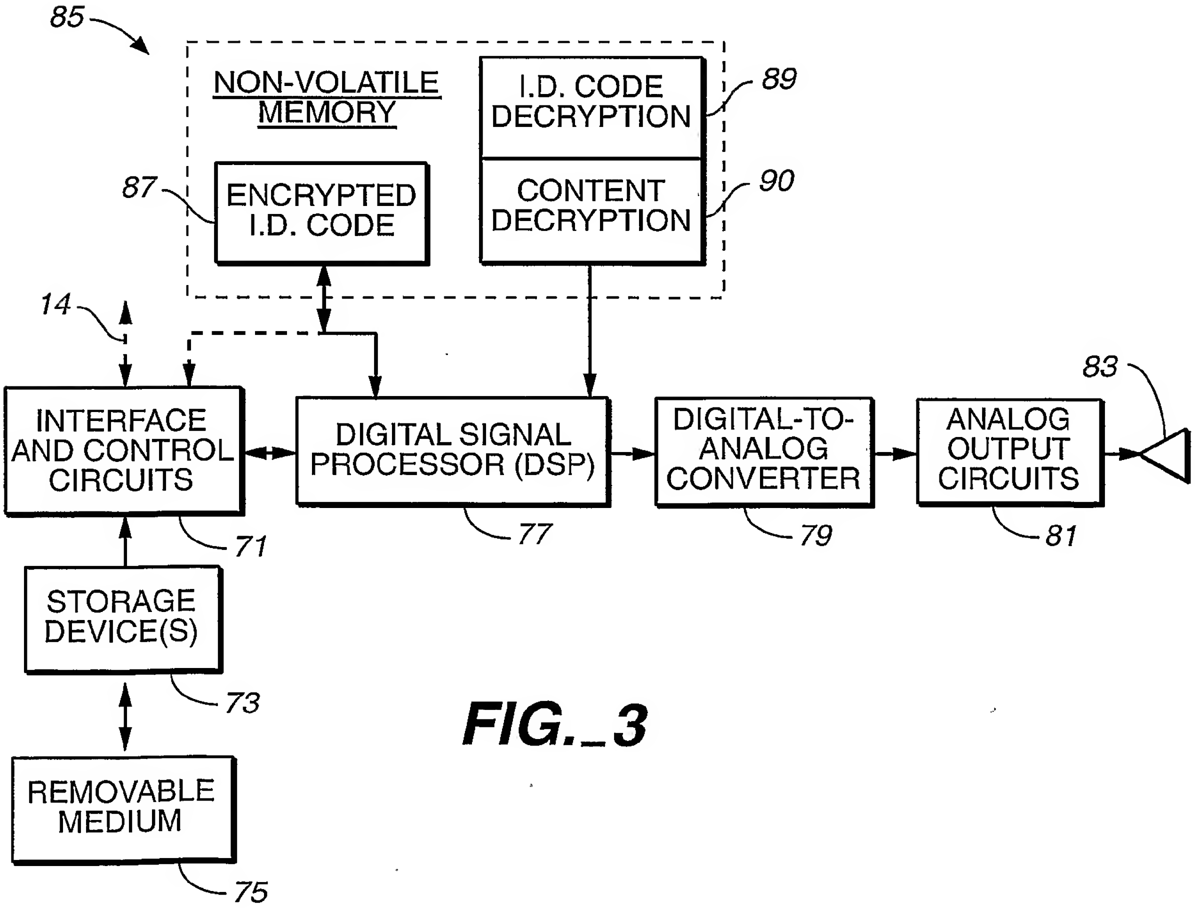

85
NON-VOLATILE MEMORY
I.D. CODE DECRYPTION
89
87
ENCRYPTED I.D. CODE
CONTENT DECRYPTION
90
14
83
INTERFACE AND CONTROL CIRCUITS
DIGITAL SIGNAL PROCESSOR (DSP)
DIGITAL-TO-ANALOG CONVERTER
ANALOG OUTPUT CIRCUITS
71
77
79
81
STORAGE DEVICE(S)
73
REMOVABLE MEDIUM
75

FIG._3

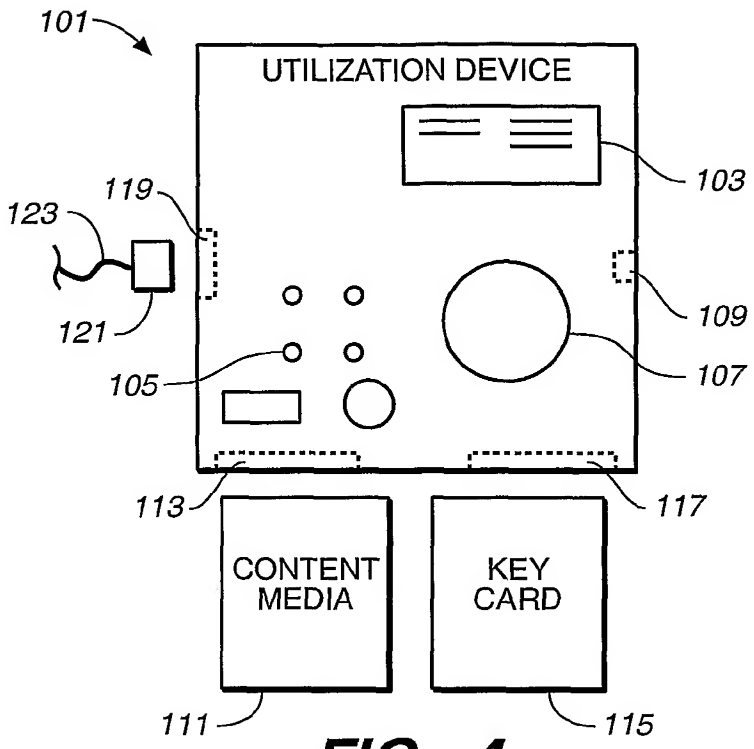

101
UTILIZATION DEVICE
103
119
123
121
109
107
105
113
117
CONTENT MEDIA
KEY CARD
111
115

FIG._4

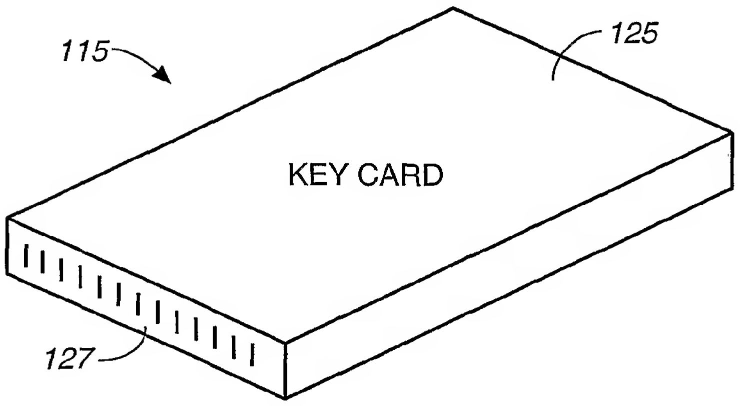

115
125
KEY CARD
127

FIG._5

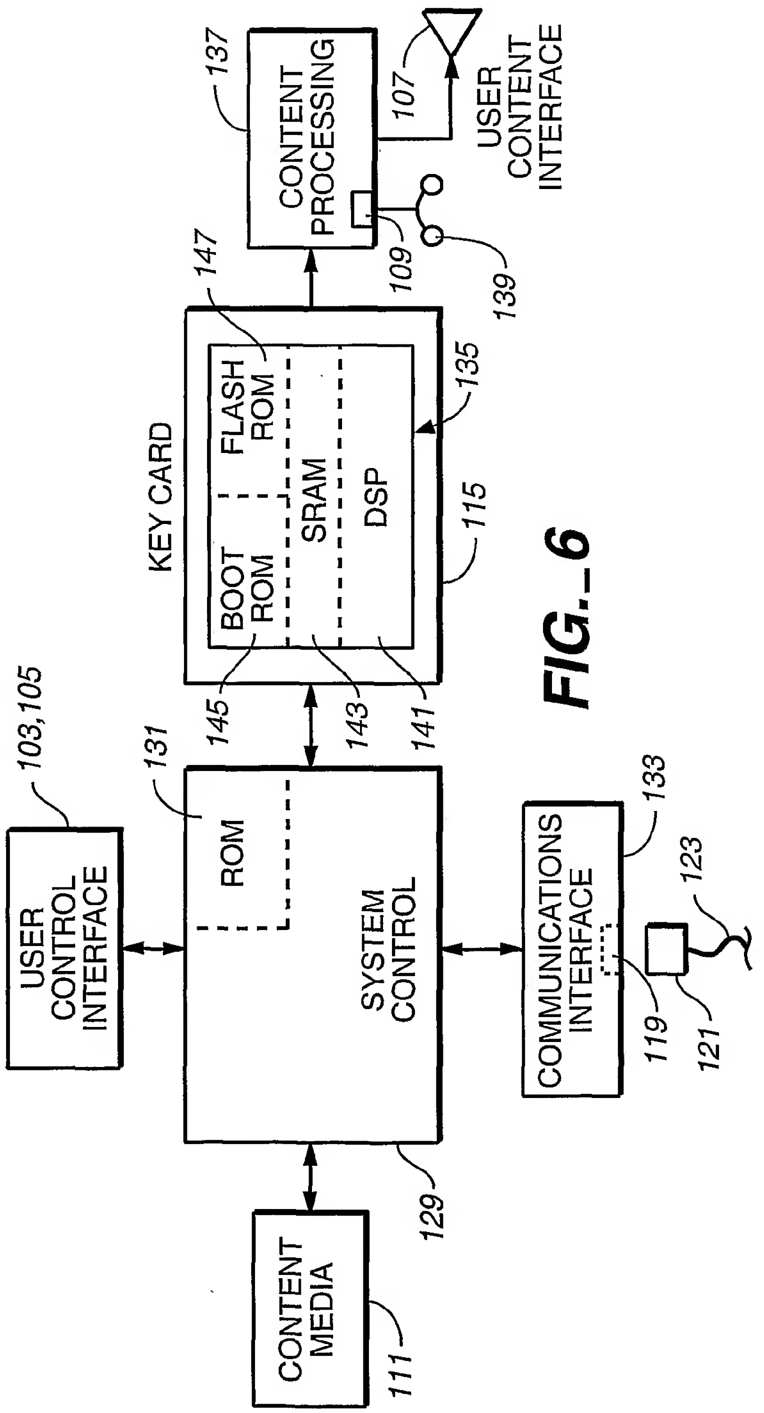

USER CONTROL INTERFACE
103,105
ROM
131
SYSTEM CONTROL
129
CONTENT MEDIA
111
COMMUNICATIONS INTERFACE
133
119
121
123
KEY CARD
BOOT ROM
FLASH ROM
SRAM
DSP
145
143
141
147
135
115
CONTENT PROCESSING
137
107
109
139
USER CONTENT INTERFACE

FIG._6

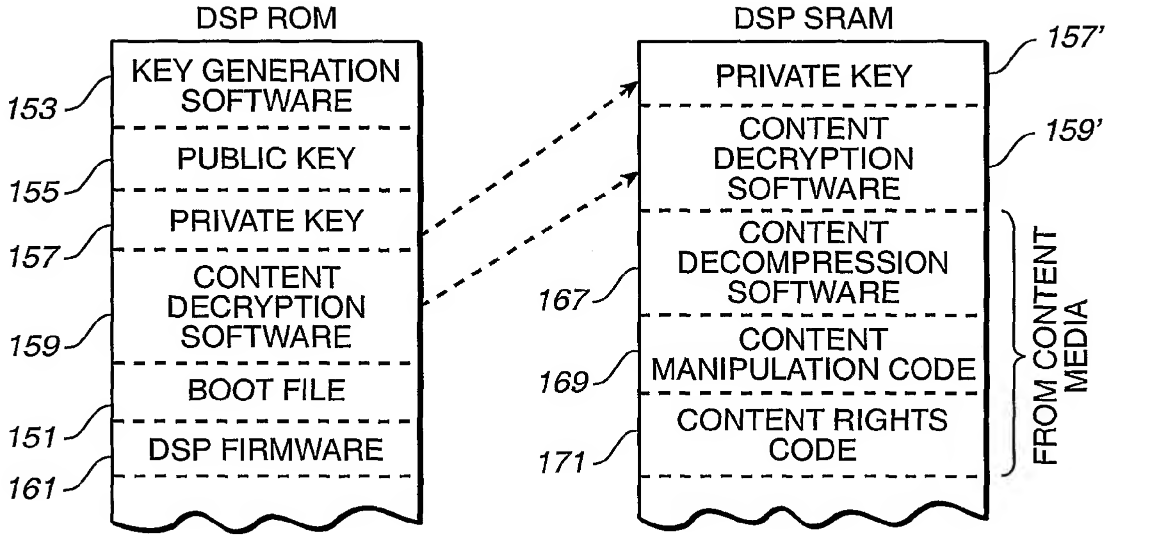


FIG._7 FIG._9

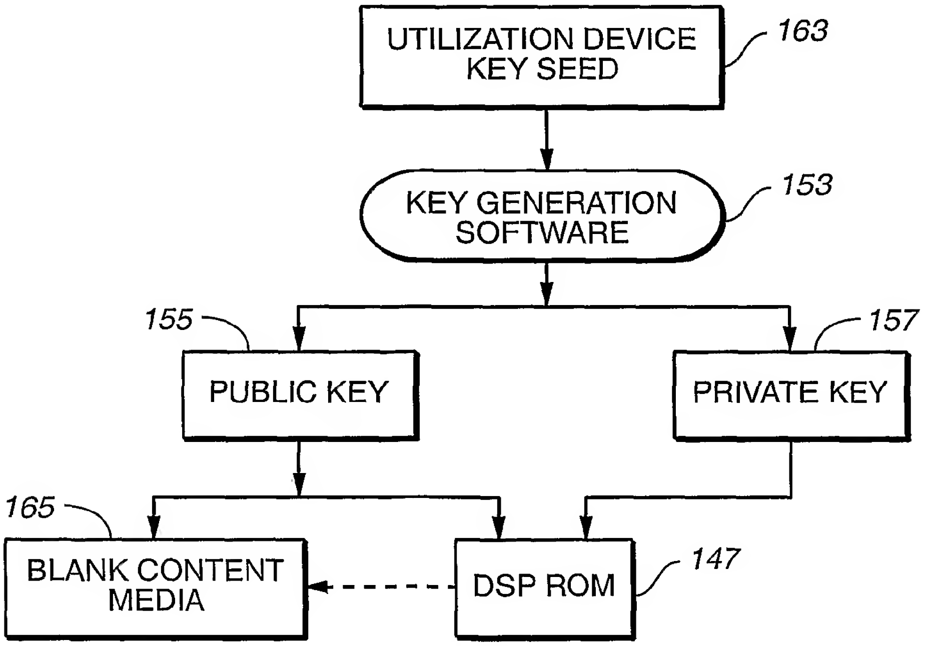


FIG._8

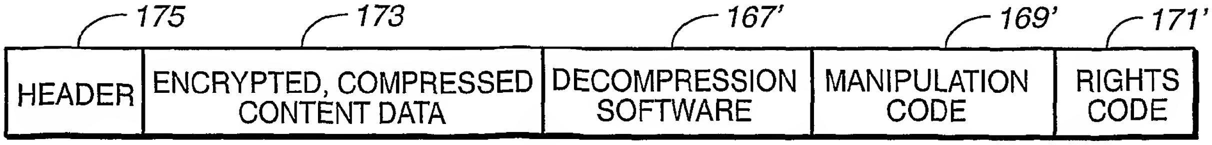


FIG._10

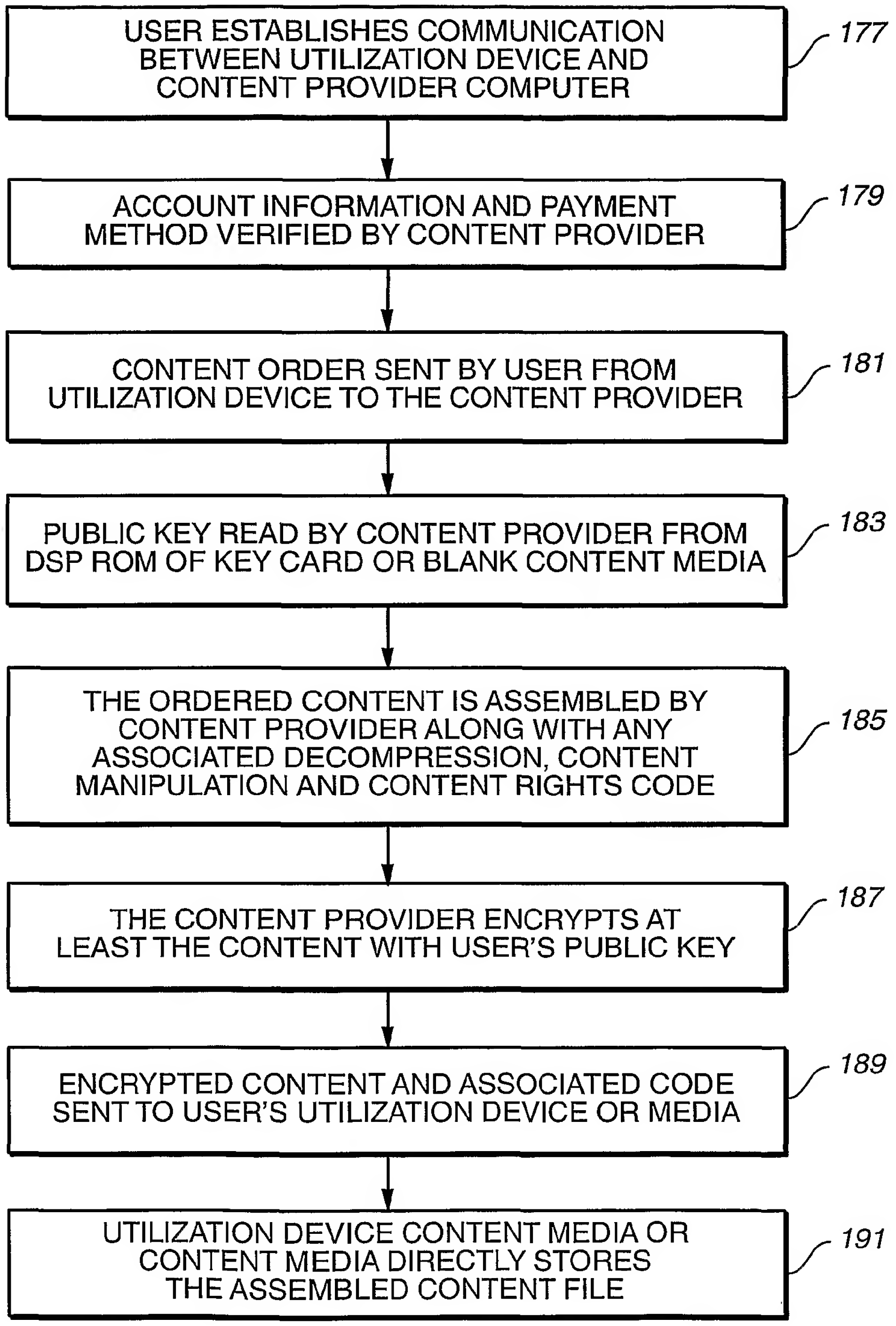

USER ESTABLISHES COMMUNICATION BETWEEN UTILIZATION DEVICE AND CONTENT PROVIDER COMPUTER
177
ACCOUNT INFORMATION AND PAYMENT METHOD VERIFIED BY CONTENT PROVIDER
179
CONTENT ORDER SENT BY USER FROM UTILIZATION DEVICE TO THE CONTENT PROVIDER
181
PUBLIC KEY READ BY CONTENT PROVIDER FROM DSP ROM OF KEY CARD OR BLANK CONTENT MEDIA
183
THE ORDERED CONTENT IS ASSEMBLED BY CONTENT PROVIDER ALONG WITH ANY ASSOCIATED DECOMPRESSION, CONTENT MANIPULATION AND CONTENT RIGHTS CODE
185
THE CONTENT PROVIDER ENCRYPTS AT LEAST THE CONTENT WITH USER'S PUBLIC KEY
187
ENCRYPTED CONTENT AND ASSOCIATED CODE SENT TO USER'S UTILIZATION DEVICE OR MEDIA
189
UTILIZATION DEVICE CONTENT MEDIA OR CONTENT MEDIA DIRECTLY STORES THE ASSEMBLED CONTENT FILE
191

FIG._11

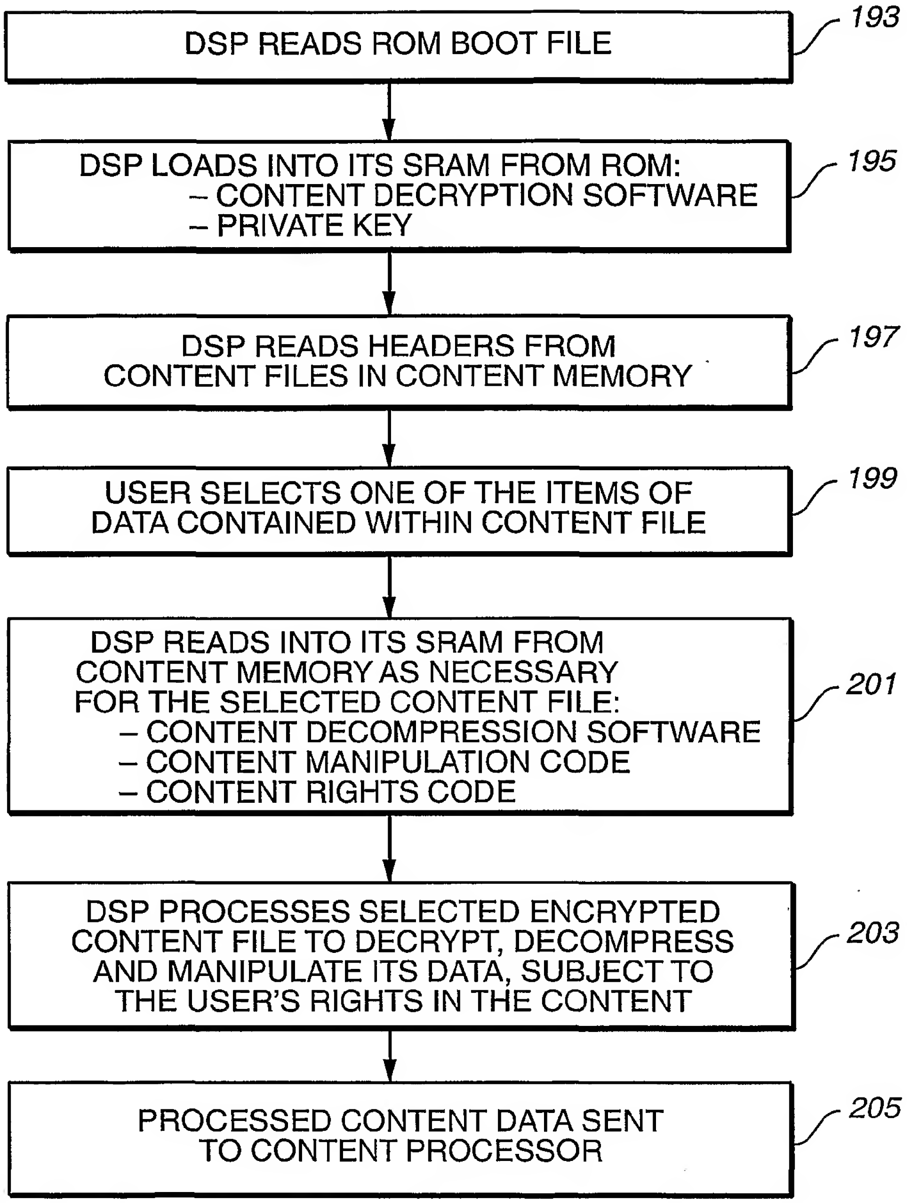

DSP READS ROM BOOT FILE
193
DSP LOADS INTO ITS SRAM FROM ROM:
– CONTENT DECRYPTION SOFTWARE
– PRIVATE KEY
195
DSP READS HEADERS FROM CONTENT FILES IN CONTENT MEMORY
197
USER SELECTS ONE OF THE ITEMS OF DATA CONTAINED WITHIN CONTENT FILE
199
DSP READS INTO ITS SRAM FROM CONTENT MEMORY AS NECESSARY FOR THE SELECTED CONTENT FILE:
– CONTENT DECOMPRESSION SOFTWARE
– CONTENT MANIPULATION CODE
– CONTENT RIGHTS CODE
201
DSP PROCESSES SELECTED ENCRYPTED CONTENT FILE TO DECRYPT, DECOMPRESS AND MANIPULATE ITS DATA, SUBJECT TO THE USER'S RIGHTS IN THE CONTENT
203
PROCESSED CONTENT DATA SENT TO CONTENT PROCESSOR
205

FIG._12

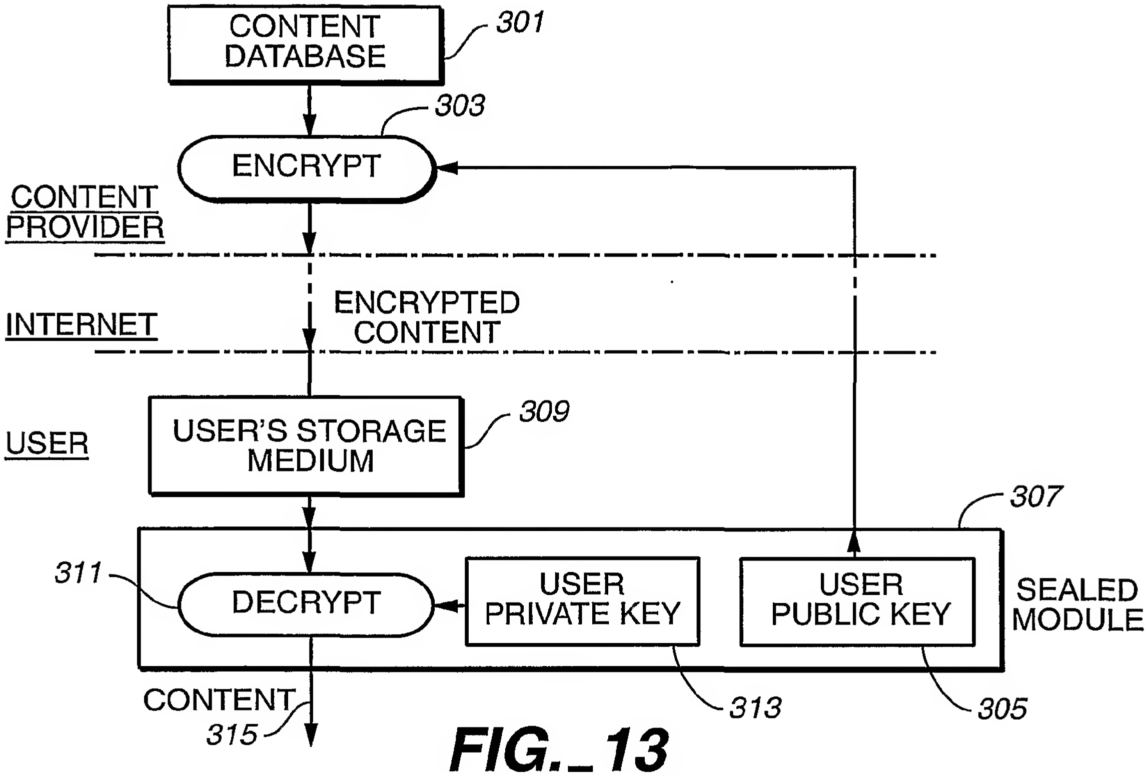

CONTENT DATABASE
301
303
ENCRYPT
CONTENT PROVIDER
INTERNET
ENCRYPTED CONTENT
USER
USER'S STORAGE MEDIUM
309
307
311
DECRYPT
USER PRIVATE KEY
USER PUBLIC KEY
SEALED MODULE
CONTENT
315
313
305

FIG._13

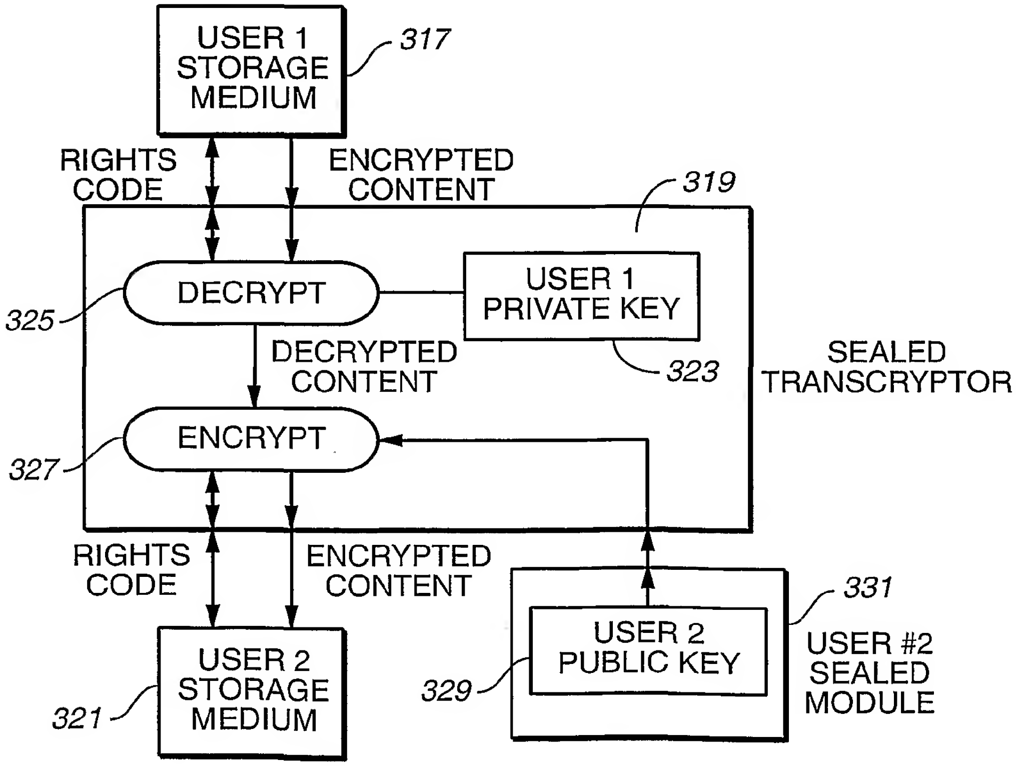

USER 1 STORAGE MEDIUM
317
RIGHTS CODE
ENCRYPTED CONTENT
319
DECRYPT
USER 1 PRIVATE KEY
325
DECRYPTED CONTENT
323
SEALED TRANSCRYPTOR
ENCRYPT
327
RIGHTS CODE
ENCRYPTED CONTENT
331
USER 2 PUBLIC KEY
USER #2 SEALED MODULE
329
USER 2 STORAGE MEDIUM
321

FIG._14

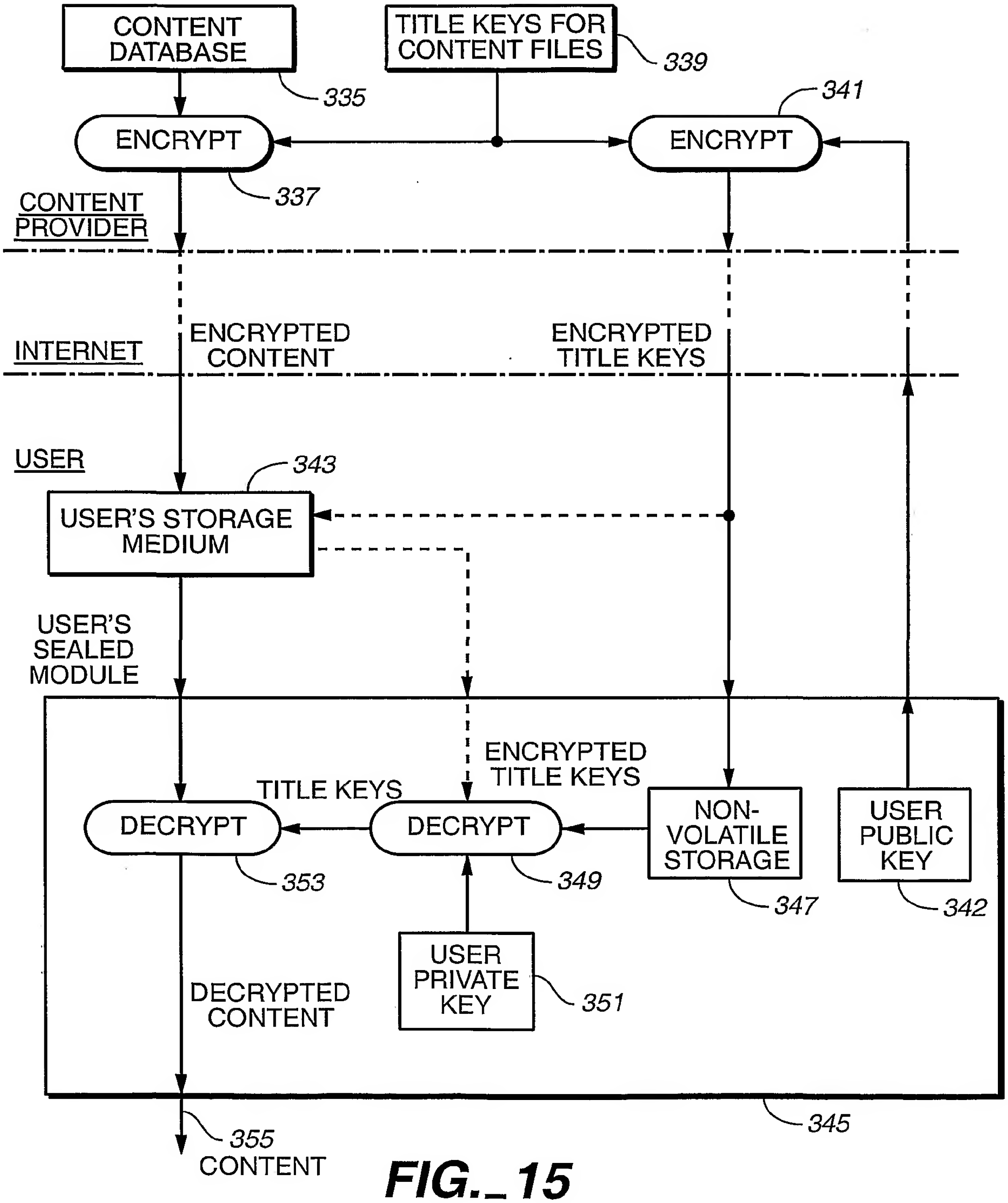

CONTENT DATABASE
335
TITLE KEYS FOR CONTENT FILES
339
ENCRYPT
337
ENCRYPT
341
CONTENT PROVIDER
INTERNET
ENCRYPTED CONTENT
ENCRYPTED TITLE KEYS
USER
343
USER'S STORAGE MEDIUM
USER'S SEALED MODULE
ENCRYPTED TITLE KEYS
TITLE KEYS
DECRYPT
353
DECRYPT
349
NON-VOLATILE STORAGE
347
USER PUBLIC KEY
342
USER PRIVATE KEY
351
DECRYPTED CONTENT
345
355
CONTENT

FIG._15

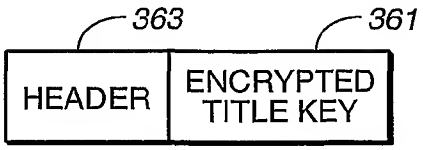


FIG._16A

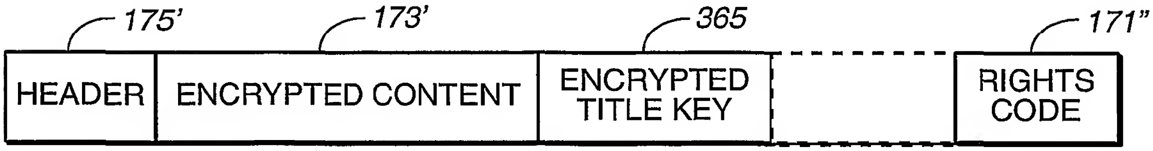


FIG._16B

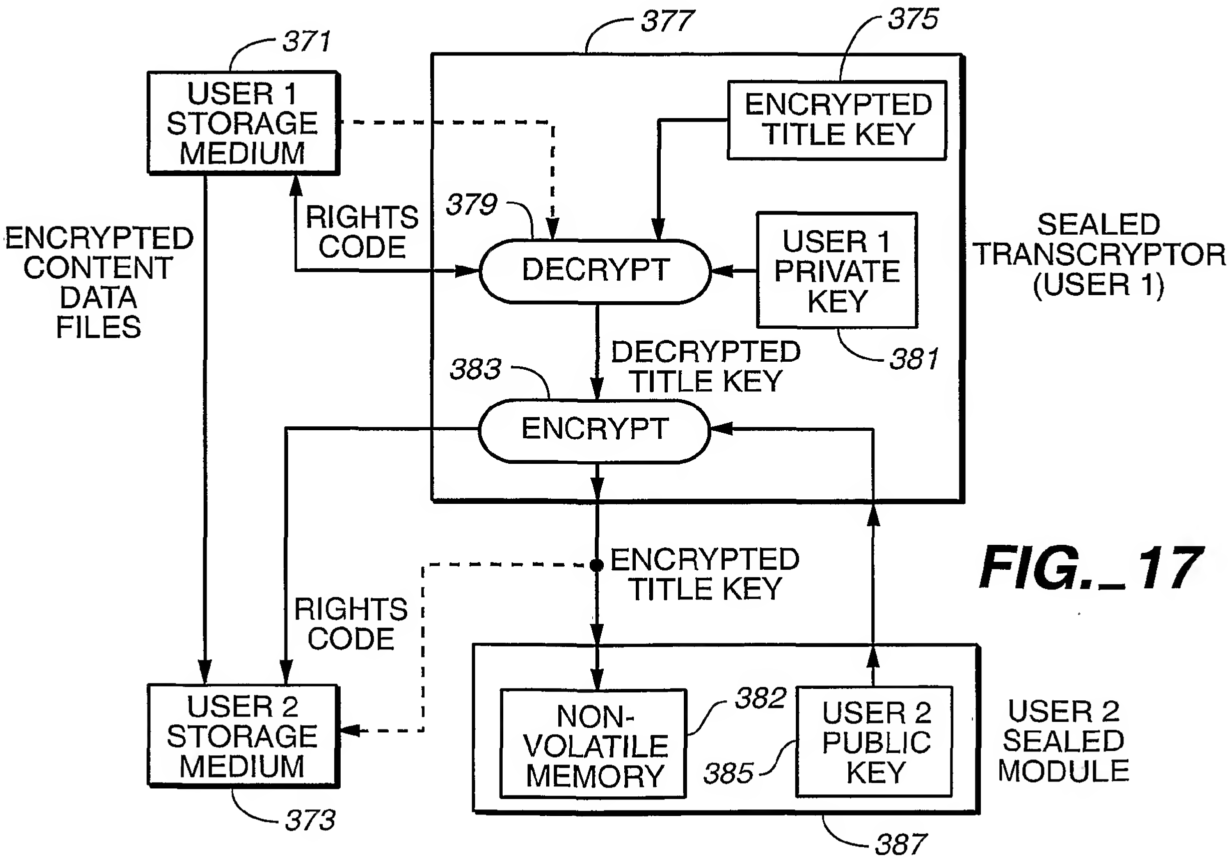


FIG._17

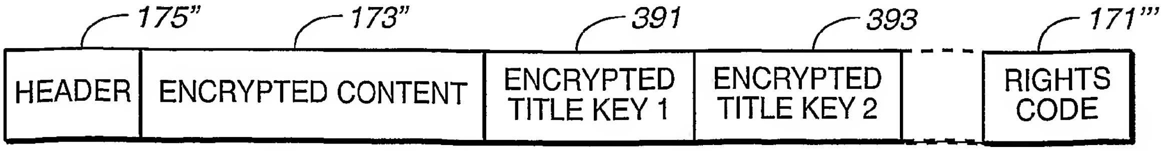


FIG._18

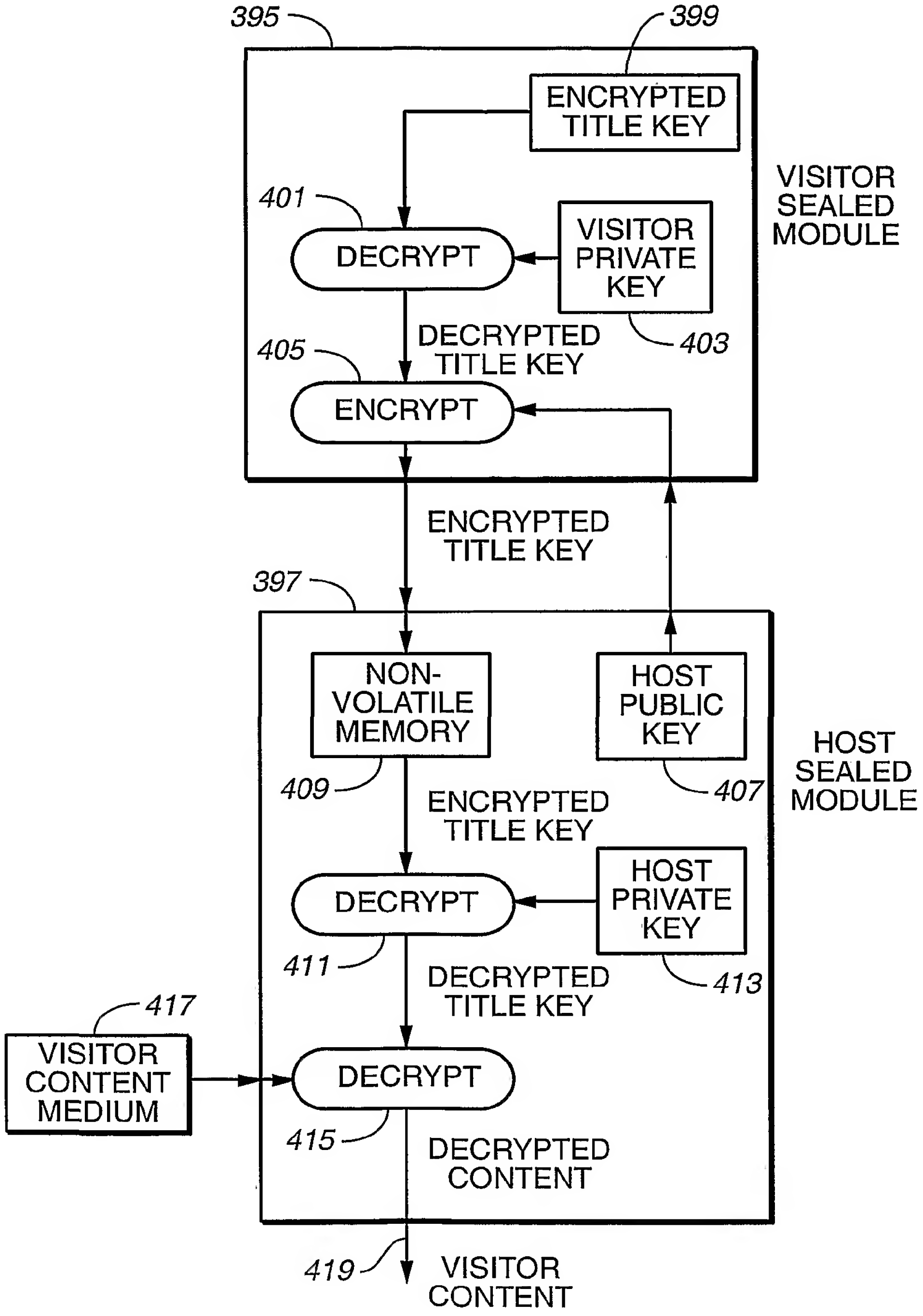

395
399
ENCRYPTED TITLE KEY
VISITOR SEALED MODULE
401
DECRYPT
VISITOR PRIVATE KEY
DECRYPTED TITLE KEY
403
405
ENCRYPT
ENCRYPTED TITLE KEY
397
NON-VOLATILE MEMORY
HOST PUBLIC KEY
HOST SEALED MODULE
409
ENCRYPTED TITLE KEY
407
DECRYPT
HOST PRIVATE KEY
411
DECRYPTED TITLE KEY
413
417
VISITOR CONTENT MEDIUM
DECRYPT
415
DECRYPTED CONTENT
419
VISITOR CONTENT

FIG._19

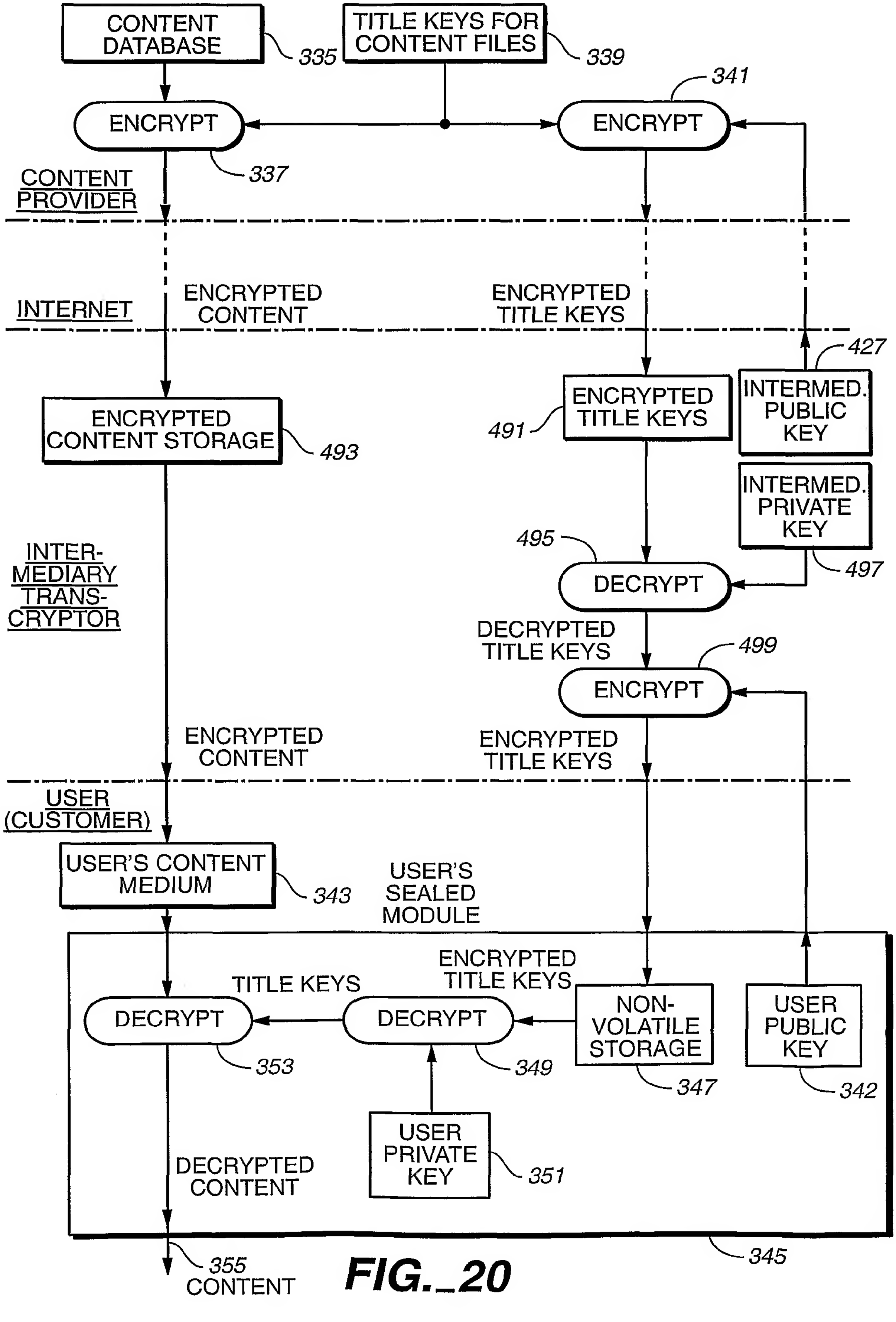
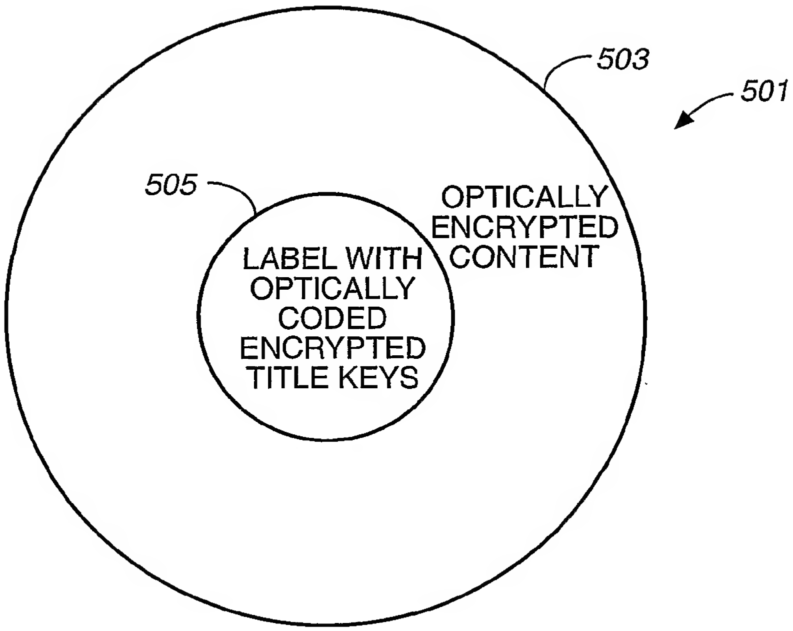

CONTENT DATABASE
335
TITLE KEYS FOR CONTENT FILES
339
341
ENCRYPT
ENCRYPT
337
CONTENT PROVIDER
INTERNET
ENCRYPTED CONTENT
ENCRYPTED TITLE KEYS
427
ENCRYPTED CONTENT STORAGE
493
491
ENCRYPTED TITLE KEYS
INTERMED. PUBLIC KEY
INTERMED. PRIVATE KEY
495
497
INTER-MEDIARY TRANS-CRYPTOR
DECRYPT
DECRYPTED TITLE KEYS
499
ENCRYPT
ENCRYPTED CONTENT
ENCRYPTED TITLE KEYS
USER (CUSTOMER)
USER'S CONTENT MEDIUM
343
USER'S SEALED MODULE
ENCRYPTED TITLE KEYS
TITLE KEYS
DECRYPT
DECRYPT
NON-VOLATILE STORAGE
USER PUBLIC KEY
353
349
347
342
USER PRIVATE KEY
351
DECRYPTED CONTENT
345
355
CONTENT

FIG._20


503
501
505
LABEL WITH OPTICALLY CODED ENCRYPTED TITLE KEYS
OPTICALLY ENCRYPTED CONTENT

COMPACT DISC

FIG._21

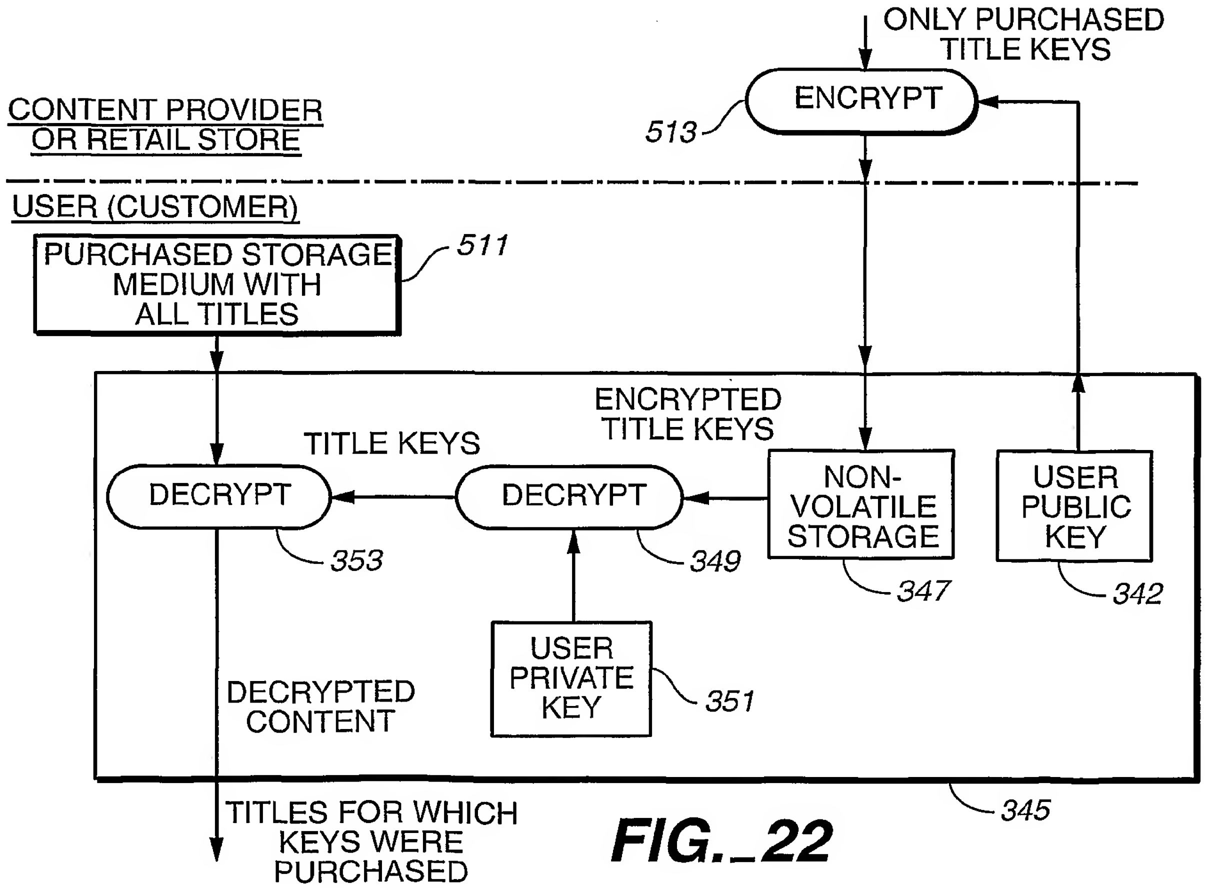


FIG._22

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

REVISED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/093000 A2

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US01/16821

(22) International Filing Date: 23 May 2001 (23.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/584,134 31 May 2000 (31.05.2000) US

(71) Applicant: ZORAN CORPORATION [US/US]; 3112 Scott Boulevard, Santa Clara, CA 95054 (US).

(72) Inventors: GOLDBERG, Paul, R.; 744 La Para Avenue, Palo Alto, CA 94306 (US). NEIDICH, Michael; 444 Saratoga Avenue, Santa Clara, CA 95050 (US).

(74) Agent: PARSONS, Gerald, P.; Skjerven Morrill Macpherson, LLP, Three Embarcadero Center, 28th Floor, San Francisco, CA 94111 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority*

(48) Date of publication of this revised version:
18 September 2003

(15) Information about Correction:
see PCT Gazette No. 38/2003 of 18 September 2003, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/093000 A2

(54) Title: SECURE ELECTRONIC INTERNET DELIVERY AND USE OF MUSIC AND OTHER VALUABLE DATA

(57) Abstract:

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and Rule 39)

Applicant's or agent's file reference M-10923-2PWO	IMPORTANT DECLARATION	Date of mailing*(day/month/year)* 28/10/2002
International application No. PCT/US 01/ 16821	International filing date*(day/month/year)* 23/05/2001	(Earliest) Priority date*(day/month/year)* 31/05/2000
International Patent Classification (IPC) or both national classification and IPC		G06F1/00
Applicant ZORAN CORPORATION		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below

1. □ The subject matter of the international application relates to:
   - a. □ scientific theories.
   - b. □ mathematical theories
   - c. □ plant varieties.
   - d. □ animal varieties.
   - e. □ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. □ schemes, rules or methods of doing business.
   - g. □ schemes, rules or methods of performing purely mental acts.
   - h. □ schemes, rules or methods of playing games.
   - i. □ methods for treatment of the human body by surgery or therapy.
   - j. □ methods for treatment of the animal body by surgery or therapy.
   - k. □ diagnostic methods practised on the human or animal body.
   - l. □ mere presentations of information.
   - m. □ computer programs for which this International Searching Authority is not equipped to search prior art.

2. ☒ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

   □ the description ☒ the claims □ the drawings

3. □ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:

   □ the written form has not been furnished or does not comply with the standard.

   □ the computer readable form has not been furnished or does not comply with the standard.

4. Further comments:

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Marja Brouwers

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 203

In view of the large number and also the wording of the claims presently on file, which render it difficult, if not impossible, to determine the matter for which protection is sought, the present application fails to comply with the clarity and/or conciseness requirements of Article 6 PCT (see also Rule 6.1(a) PCT) to such an extent that a meaningful search is impossible. Consequently, no search report can be established for the present application.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.